HMD (2022) 59:1366–1379
https://doi.org/10.1365/s40702-022-00903-7

SCHWERPUNKT

Wahrung der Privatsphäre in einer Blockchain-basierten Plattform: Anwendung für MRO-Dokumentationen der Luftfahrtindustrie

Jan Zedel · Natalia Kliewer

Eingegangen: 13. Mai 2022 / Angenommen: 14. August 2022 / Online publiziert: 5. September 2022

Zusammenfassung MRO-Dokumentationen (MRO, deutsch: Wartung, Reparatur und Instandsetzung) der Luftfahrtindustrie sind notwendig, um die Flugtauglichkeit von Flugzeugersatzteilen zu zertifizieren und den Handel mit Teilen auf dem Sekundärmarkt zu ermöglichen. Da Dokumente wettbewerbsrelevante Daten enthalten können, werden diese vertraulich behandelt. Dennoch besteht die Verpflichtung, die Validität von Dokumentationshistorien gegenüber Behörden und Handelspartnern nachzuweisen.

Die Dokumentationspraxis ist durch analoge Erfassung sowie unterschiedliche Prozesse und Systeme geprägt. Dieser Umstand erhöht die Fehleranfälligkeit und Manipulierbarkeit von Dokumenten. Eine standardisierte Datenerfassung sowie der Einsatz eines einheitlichen Systems könnten zur Optimierung der Prozesse beitragen.

Öffentliche Blockchains und der Einsatz von Smart-Contract-Systemen gewährleisten die Datenintegrität, ohne dass sich die Netzwerkteilnehmer gegenseitig vertrauen müssen. Durch automatische Überprüfung von Verträgen oder Dateneingaben können Fehler leicht identifiziert werden. Anreizsysteme erschweren zudem die Manipulation gespeicherter Daten und erhöhen deren Persistenz im System.

Die Transparenz öffentlicher Netzwerke behindert die Adaption der Blockchain-Technologie zur Verbesserung der MRO-Dokumentationsprozesse. Ein Zielkonflikt entsteht aus der Unvereinbarkeit von Privatsphäre-Anforderungen einerseits und den Spezifikationen öffentlicher Blockchain-Netzwerke andererseits. Private oder konsortiale Blockchain-Anwendungen stellen einen Kompromiss dar, lösen das Problem aber nicht.

Jan Zedel (✉) · Natalia Kliewer
Fachbereich Wirtschaftswissenschaft, Professur für Wirtschaftsinformatik, Freie Universität Berlin, Garystraße 21, 14195 Berlin, Deutschland
E-Mail: jan.zedel@fu-berlin.de

Natalia Kliewer
E-Mail: natalia.kliewer@fu-berlin.de

Dieser Artikel folgt einem Design Science Research (DSR) Ansatz und stellt die Infrastruktur einer Blockchain-basierten Plattform für die MRO-Branche vor, die eine Lösung des beschriebenen Zielkonfliktes für den Anwendungsfall adressiert und damit die Grundlage für eine standardisierte Dokumentationspraxis bildet. Berücksichtigte Anforderungen und Designprinzipien sowie die abgeleiteten technischen Spezifikationen erläutern allgemein, wie Daten in Blockchain-basierten Plattformen vertraulich geteilt und validiert werden können.

Schlüsselwörter Blockchain · Dokumentationsprozesse · Luftfahrtindustrie · MRO · Plattform

Maintaining Privacy in a Blockchain-based Platform: Application to Aviation Industry MRO Documentation

Abstract Aviation industry MRO (MRO: maintenance, repair and overhaul) documentation is necessary to certify aircraft spare parts' airworthiness and allow parts to be traded on the secondary market. Since the documents may contain competitively sensitive data, they are treated confidentially. Nevertheless, there is an obligation to demonstrate the validity of documentation histories to authorities and trading partners.

Documentation practice is characterized by analog recording and varying processes and systems. This circumstance increases the susceptibility to errors and manipulation of documents. Standardized data capture and a unified system could help optimize processes.

Public blockchains and smart contract systems ensure data integrity without needing network participants to trust each other. Errors can be easily identified through automatic verification of contracts or data entries. Incentive systems also make it challenging to manipulate stored data and increase its persistence in the system.

The transparency of public networks hinders the adaptation of blockchain technology to improve MRO documentation processes. A trade-off arises from the incompatibility of privacy requirements on the one hand and the specifications of public blockchain networks on the other. Private or consortium blockchain applications represent a compromise but do not solve the problem.

This article follows a DSR approach and presents the infrastructure of a blockchain-based platform for the MRO industry that addresses a solution to the described trade-off for the use case and thus forms the basis for a standardized documentation practice. Considered requirements and design principles, as well as the derived technical specifications, explain in general terms how data can be confidentially shared and validated in blockchain-based platforms.

Keywords Blockchain · Documentation processes · Aviation industry · MRO · Platform

1 Problembeschreibung und Methodik

Dokumentationspraktiken der Luftfahrt MRO-Branche sind durch einen hohen Anteil analoger Erfassung gekennzeichnet. Wird ein Bauteil repariert, werden Zertifizierungen und Belege meist in Papierform erstellt und versandt. Für die digitale Erfassung und Verarbeitung von Dokumenten gibt es keinen einheitlichen Standard. Insbesondere für komplexe Bauteile oder Flugzeuge ist das Dokumentenmangement sehr aufwendig. Fehlende Standards führen zu Intransparenz sowie Verlust- und Fehleranfälligkeit. Sobald Unregelmäßigkeiten in einer Dokumentation existieren verliert ein Bauteil die Flugtauglichkeit und darf nicht weiterverwendet werden. Zur Überpfüng von Zertifikaten müssen MRO-Betriebe Einsicht in Dokumente ermöglichen. Da Dokumentationen sensible und wettbewersrelevante Daten beinhalten können, ergeben sich hohe Sicherheitsanforderungen bei der Weitergabe von Informationen. (Efthymiou et al. 2022).

Die hier vorgstellten Forschungsergebnisse sind Teil des RAPADO Forschungsprojektes, bei dem ein Rahmenwerk geschaffen wird, welches die authentifizierte, verschlüsselte und validierte Ablage von Dokumentationen von Flugzeugersatzteilen zur Standardisierung durch die Aufsichtsbehörden ermöglichen und somit eine Lösung genannter Probleme bereitstellen soll.

Als Vorarbeit zum RAPADO Projekt haben Wickboldt und Kliewer bereits die Speicherung von Daten auf einem verteilten Ledger vorgeschlagen, um die Intransparenz bei der Dokumentation von Werkstattereignissen zu verringern (Wickboldt und Kliewer 2018). In einem Konsortium-Netzwerk könnten MRO-Marktteilnehmer vertrauliche Daten authentifiziert austauschen und dabei auf eine gemeinsame und konsistente Datenbasis zugreifen, die Grundlage für die Optimierung von Geschäftsprozessen bilden kann (Wickboldt und Kliewer 2019). Andere Quellen empfehlen die Verwendung öffentlicher Netzwerkstrukturen, sofern Privatsphäre nicht gewahrt bleiben muss (Hasan et al. 2020). Auf diese Weise ließe sich ein hohes Maß an Datenpersistenz und -integrität erreichen, ohne das Teilnehmer einem zentralen Betreiber vertrauen müssen. Weiterhin wurden in der Industrie Konzepte für Dokumentationsplattformen erprobt, die auf private bzw. konsortiale Infrastruktur setzen, wie Honeywell oder SITA.

Bei der Implementierung von Blockchain-Anwendungen im Unternehmensumfeld spielt die Wahl der Infrastruktur und damit auch der Grad der Dezentralisierung eine entscheidende Rolle. Denn die ursprünglichen Anwendungszwecke einer Blockchain, ein ohne Vertrauen funktionierendes Peer-to-Peer Netzwerk mit einem hohen Maß an Datenpersistenz und -integrität (Nakamoto 2008), lassen sich in privaten Netzwerken nicht hinreichend realisieren (Buterin 2015). Dies wird an dem Beispiel Tradelens deutlich, einer Plattform zur Abwicklung von Containerlogistik. Trotz erfolgreicher Anwendung steht die Plattform in der Kritik, da eine zu starke Zentralisierung und Steuerung von Seiten der Firma Maersk der Standardisierung und Entwicklung kritischer Infrastruktur im Wege steht (Lohmer und Lasch 2020). Gleichzeitig ist die Wahrung der Privatsphäre für sensible Geschäftsdaten Grundvoraussetzung für Unternehmen, um an einem verteilten Netzwerk zu partizipieren (Holbrook 2020). Privatsphäre in öffentlichen Blockchain-Netzwerken stellt somit

eine große Herausforderung für die Adaption im Unternehmenskontext dar (Buterin 2016).

Die Analyse bisheriger Konzepte der Luftfahrt-MRO-Branche zeigt, dass die Verwendung privater Netzwerke bevorzugt wird (Aleshi et al. 2019; Schyga et al. 2019; Wickboldt und Kliewer 2019). Dabei wurden Vor- und Nachteile zentraler und dezentraler Infrastrukturen erkannt (Hasan et al. 2020). Um einen von der Industrie akzeptierten Standard zu schaffen scheint es erforderlich, dass eine Dokumentationsplattform die Anforderungen der MRO-Branche umfänglich erfüllt. Bei der Verwendung von Distributed-Ledger-Technologien für den Anwendungsfall stellt sich die Frage, wie eine Infrastruktur die Mehrwerte Datenpersistenz und -Integrität mit den Anforderungen an Sicherheit und Privatsphäre in Einklang bringen kann.

Die hier vorgestellten Forschungsergebnisse basieren auf einem Design Science Research (DSR) Ansatz nach Hevner et al. (2004) und haben zum Ziel, präskriptives Wissen zur Erstellung einer Blockchain-basierten-Infrastruktur für den Anwendungsfall zu beschreiben. Das Vorgehen folgt einem generischen DSR-Forschungsprozess (Gleasure 2013), bei dem eine Relation zwischen Problem und Lösungsbeschreibung hergestellt und somit nach Defintion von Venable (2006) zum Design-Wissen der Domäne beigetragen wird. Dabei werden zunächst Anforderungen identifiziert und präzisiert, um anschließend unter Verwendung von Designprinzipien den Lösungsraum interativ einzugrenzen. Zur Lösung von auftretenden Konflikten werden weiterführende Konzepte herangezogen und angewandt, was eine neuartige Ergänzung initialer Designprinzipien für die Anwendungsdomäne darstellt. Die Ergebnisse werden durch die Beschreibung der Infrastruktur formalisiert und anschließend durch Überprüfung der Anforderungserfüllung validiert. Die Ergebnisdarstellung ist gemäß vom Brocke und Maedche (2019) in sechs verschiedene Dimensionen gegliedert. Die Systematik des DSR-Grids unterteilt die inhaltliche Darstellung wie folgt:

Problembeschreibung Sowohl im akademischen als auch im industriellen Bereich sind Proof of Concepts (POCs) beschrieben, die mit Hilfe von Blockchain-Plattformen Probleme der MRO-Dokumentationsprozesse lösen sollen. Probleme bisheriger Konzepte ergeben sich daraus, dass insbesondere die Anforderungen Datenpersistenz und -integrität nicht mit erforderlicher Wahrung der Privatsphäre in Einklang gebracht sind.

Methodik Das Vorgehen zur Konzeptionierung der Zielarchitektur folgt einem Design Science Research Ansatz. Die Ergebnisdarstellung erfolgt in einem DSR-Grid und beabsichtigt die Generierung von Design-Wissen im Bereich Plattformentwicklung einer Blockchain-basierten Lösung zur Optimierung von MRO-Dokumentationsprozessen.

Eingangswissen Die im Laufe des Projektes erhobenen Anforderungen für eine MRO-Plattformlösung sowie generelle Designprinzipien zur Implementierung von Blockchain-Anwendungen im Unternehmenskontext bilden das Basiswissen zur Konzeptionierung einer Zielarchitektur.

Konzepte Um Privatsphäre zu gewährleisten und gleichzeitig die Programmierbarkeit von Blockchain-Anwendung zu ermöglichen, können verschiedene Technologien des sogenannten Off-Chainings verwendet werden. Die Anwendung ermöglicht eine vertrauensvolle Datenverarbeitung in privater Umgebung. Mit Hilfe des Off-Chainings werden Zielkonflikte spezifizierter Designprinzipien für den Anwendungsfall gelöst.

Lösungsbeschreibung Die Zielarchitektur umfasst die Verwendung von drei Netzwerken, einem öffentlichen Blockchain-Netzwerk, einem verteilten Dateisystem sowie einem für den Anwendungsfall konzipierten Off-Chain-Validierungsnetzwerkes. Zudem umfasst die Lösung ein Konzept zur Verschlüsselung und Verwendung von Smart Contracts, zur Implementierung des sicheren Datenaustauschs sowie der Geschäftslogik des Anwendungsfalls. Designentscheidungen sind in der Lösungsbeschreibung begründet.

Ausgangswissen Anhand einzelner Prozesse im System ist die Anforderungserfüllung der Zielarchitektur dargelegt. Die Lösungsdomäne bildet das generierte Design-Wissen.

2 Eingangswissen – Anforderungserhebung für eine MRO-Dokumentationsplattform

Anforderungen an eine MRO-Dokumentationsplattform ergeben sich aus Marktgegebenheiten und bestehenden Prozessen. Hierzu haben Wickboldt und Kliewer (2018) bereits die Kernanforderungen: persistente Datenhaltung, selektive Zugriffsbeschränkung, Gewährleistung der Datenintegrität sowie Transparenz der Dokumentationshistorien, erhoben. Darauf aufbauend wurden Anforderungen im Forschungsprojekt RAPADO erneut ermittelt und detaillierter beschrieben. Die Erhebung erfolgte in mehreren aufeinanderfolgenden Workshops mit Experten der MRO-Branche, unter Durchführung von Interview-Reihen und Prozessanalysen. Befragte Experten sind drei Kategorien von Marktteilnehmern zuzordnen: MRO-Werkstattbetriebe, MRO- Teile-Händler und Airlines. Neben der Präzisierung der Anforderungen von Wickboldt und Kliewer (2018) wurde zusätzlich die Einhaltung des Datenschutzes explizit definiert. Nachfolgende Anforderungen geben den Rahmen vor, in dem Designprinzipien und weiterführende Konzepte bei der Definition der Zielarchitektur spezifiziert werden.

1. Persistente Datenhaltung: Im Gegensatz zu bisherigen Anwendungen/Praktiken der MRO-Branche müssen Dokumente unter allen Umständen dauerhaft gespeichert werden und jederzeit zugänglich sein. Eine persistente Datenhaltung muss die langfristige Überprüfbarkeit von Dokumenten für Marktteilnehmer, wie zum Beispiel Regulierungsbehörden, ermöglichen, um die Manipulierbarkeit und Fehleranfälligkeit von Daten zu reduzieren.
2. Einhaltung des Datenschutzes/Wahrung der Privatsphäre: Viele MRO-Dokumente beinhalten wettbewerbsrelevante oder personenbezogene Daten und unterliegen

somit einer besonders hohen Anforderung an Vertraulichkeit. Dementsprechend dürfen Daten nicht frei zugänglich sein. Weiterhin muss die Übertragung der Daten verschlüsselt sein.

3. Selektive Zugriffsbeschränkung: Daten sollen nur bei selektiv gewährter Freigabe durch den Eigentümer der Daten oder bei Vorliegen eines Zwischenfalls durch Regulierungsbehörden einsehbar sein. Die selektive Zugriffsbeschränkung stellt einen wichtigen Faktor für die Akzeptanz der Lösung dar, da MRO-Betriebe Kontrolle über ihre Daten behalten wollen.
4. Gewährleistung der Datenintegrität: Um die Korrektheit sämtlicher Dokumente zu überprüfen ist die Implementierung eines Validierungs-mechanismus erforderlich. Dabei muss sichergestellt werden, dass die Validierung eine fehlerfreie Überprüfung von Dokumenten ermöglicht, die sicher gegenüber Manipulationen und unautorisierten Einsichten ist. Zusätzlich muss die Unabhängigkeit der validierenden Instanz gewährleistet sein.
5. Transparenz der Dokumentationshistorien: Dokumentationshistorien müssen eindeutig Prozessen oder Bauteilen zuzuordnen sein und die Geschäftslogik widerspiegeln. Um eine entsprechende Zuordnung zu gewährleisten muss eine Bauteil-Dokumenten-Hierarchie geschaffen werden. Bei Bedarf müssen Dokumentationshistorien für andere Nutzer einsehbar oder übertragbar sein.

3 Eingangswissen – Designprinzipien

Bei der Entwicklung von Blockchain-Anwendungen für Unternehmenszwecke gilt es Designprinzipien zu beachten. Die Prinzipien ergeben sich aus inhärenten Eigenschaften der Technologie und dessen Anwendungszweck. Bezüglich des Entwurfes der Infrastruktur im Unternehmensumfeld sind nach Holbrook (2020) folgende Prinzipien von Relevanz: Datenpersistenz/-integrität, Verfügbarkeit, Transparenz, Sicherheit und Privatsphäre. Im Folgenden werden die Implikationen dieser Prinzipien für eine Implementierung von Blockchain-Anwendungen dargestellt. Anschließend werden resultierende Zielkonflikte der Prinzipien diskutiert. Die entsprechende Ausgestaltung für den Anwendungsfall zeigt sich in der Lösungsbeschreibung.

Datenpersistenz/-integrität Bei einer Blockchain handelt es sich um einen verteilten Datensatz, dessen Daten chronologisch gespeichert und kryptografisch miteinander verknüpft sind. Im Gegensatz zum klassischen Client-Server-Modell, bei dem es meist eine zentrale Instanz gibt, werden Daten über alle Knoten im Netzwerk synchronisiert. Je größer das Netzwerk und damit der Grad der Dezentralisierung ist, desto höher ist die Wahrscheinlichkeit, dass Daten dauerhaft im Netzwerk verbleiben. Konsensmechanismen prüfen die Legitimität von Statusän derungen. Je aufwendiger die Teilhabe an dem Konsensfindungsprozess ist und je mehr Instanzen daran partizipieren, desto sicherer ist das Netzwerk gegenüber Kompromittierung. Der Entwurf von Unternehmensanwendungen zielt oft auf Datenpersistenz und nicht-Manipulierbarkeit von Daten ab. Bei diesem Designprinzip handelt es sich folglich um eine Funktion die vom Grad der Dezentralisierung und dem Konsensmechanismus abhängig ist.

Verfügbarkeit Verteilte Netzwerke helfen dabei die Verfügbarkeit von Daten oder digitalen Dienstleistungen zu erhöhen. Unter der Voraussetzung das Daten stets synchronisiert sind, können Redundanzen und Replikation einzelne Fehlerquellen und damit den Ausfall von kritischer Infrastruktur kompensieren. In Hinblick auf Blockchain-Anwendungen muss bedacht werden, dass sich eine hohe Verfügbarkeit dann ergibt, wenn viele Netzwerkknoten existieren und keine zentrale Instanz Funktionalitäten bündelt. Eine Bündelung kann entstehen, wenn ein Netzwerk zugriffsbeschränkt ist und eine selektive Auswahl der Teilnehmer oder eine klare Zuteilung von Rollen und Funktionen vorliegt. Zusätzlich kann die Schaffung von Redundanzen auf andere Ebenen ausgeweitet werden, wie zum Beispiel die Datenspeicherung in Off-Chain Dateisystemen.

Transparenz Im Gegensatz zu der Wahrung der Privatsphäre kann eine Kernanforderung die Herstellung von Transparenz sein. Für private bzw. konsortiale Blockchains mit einem zentralen Zugriffsmanagement können beide Anforderungen leicht in Einklang gebracht werden, da Daten nur in einem ausgewählten Kreis zur Verfügung gestellt werden. Im Allgemeinen eignet sich eine Blockchain für die Herstellung von Datentransparenz ideal. Durch die Synchronisation des Status und Replizierung von Daten über mehrere Knoten können Prozessdaten mit Stakeholdern geteilt werden. Als Datenstruktur liegt der Blockchain ein Hash-Baum zugrunde, wodurch Änderungen leicht zu identifizieren sind, was die Analyse chronologisch sequentiell gespeicherter Daten vereinfacht. Gleichzeitig stellt Blockchain eine Authentizitätslösung dar, welche die Echtheit von Daten und zugehöriger Absender garantieren kann.

Sicherheit und Privatsphäre Der Sicherheit und Privatsphäre kommt im Unternehmenskontext eine besonders hohe Bedeutung zu. Der Begriff Sicherheit wird manchmal mit Datenintegrität gleichgesetzt, bezieht sich im Unternehmensumfeld aber meist auf die selektive Vergabe von Zugriffsrechten bzw. den Schutz der Daten vor unautorisierten Zugriffen und Kompromittierung. Potenzielle Geschäftsgeheimnisse müssen gewahrt bleiben sowie die Datenschutzrichtlinien eingehalten werden. Um das Risiko von Angriffsvektoren gering zu halten, werden oft private bzw. konsortiale Blockchains implementiert, deren Zugriffsrechte zentral für autorisierte Nutzer verwaltet werden. Bei der Verwendung öffentlicher Infrastruktur ist zu bedenken, dass Nutzer-Accounts nicht anonym, sondern lediglich pseudonymisiert sind. Entsprechend sollten sensible Daten niemals in Klartext auf einer öffentlichen Blockchain gespeichert werden. Für öffentliche Netzwerke müssen andere Technologien bemüht werden um die Privatsphäre herzustellen, wie zum Beispiel Verschlüsselung, Zero-Knowledge-Proofs, Secure Multiparty Computation (sMPC) u. a.

Zielkonflikte Die Berücksichtigung mehrerer Designprinzipien kann zu Konflikten bei der technischen Umsetzung führen. Datenpersistenz, Verfügbarkeit und Transparenz lassen sich am besten in öffentlichen Netzwerken realisieren. Jedoch gewährleisten private Netzwerke mehr Sicherheit und Privatsphäre. Zwar gehen konsortiale Netzwerke einen Mittelweg, bei dem versucht wird die Mehrwerte zu vereinen, jedoch kommen diese Netzwerke selten ohne zentrale Instanzen aus. Zum

einen bilden zentrale Instanzen „Single-Point-Of-Failures“ und somit potenzielle Angriffsvektoren. Zum anderen können sich Ineffizienzen und Interessenskonflikte zwischen partizipierenden Parteien ergeben. In existierenden Blockchain-Anwendungen im Unternehmenskontext konnte beobachtet werden, dass genannte Konflikte zu Akzeptanzverlust der Plattform innerhalb des Konsortiums führen können (Beispiel Tradelens).

4 Konzepte – Privatsphäre in öffentlichen Blockchain-Netzwerken

Etablierte Netzwerke, die Privatsphäre für öffentliche Blockchain-Netzwerke garantieren, wie zum Beispiel ZCash und Monero, arbeiten mit verifizierenden Berechnungen. Diese Plattformen bieten allerdings nicht die Programmierbarkeit Smart Contract fähiger Blockchains, wie zum Beispiel Ethereum, und sind darauf ausgelegt Datenschutz für bestimmte Klassen von Anwendungen zu gewährleisten, z. B. Zahlungsverkehr.

Eine theoretisch ideale Lösung ist die sichere kryptografische Verschleierung (Manjunath et al. 2019). Dabei ist das Ziel Programme in eine Black Box zu verwandeln, die zwar einer klaren Logik folgt und eindeutige wiederholbare Ergebnisse liefert, aber deren Funktionsweise kryptografisch verschleiert wird. Jedoch ist die perfekte Verschleierung mathematisch unmöglich (Barak et al. 2012). Ein geringerer Sicherheitsstandard, der Anforderungen hinreichend erfüllen könnte, ist aktuell noch sehr rechenintensiv (Garg et al. 2013) und damit nicht nutzbar für Blockchain-Anwendungen.

Um dennoch die Privatsphäre in öffentlichen Blockchain-Anwendungen zu wahren, müssen selektive Daten an externe Ressourcen ausgelagert und abseits der Blockchain berechnet werden. Damit die Vertrauenwürdigkeit externer Berechnungen maximiert wird, kommen Konzepte des Off-Chainings zum Einsatz. Einem Modell von Eberhardt und Heiss (2018) folgend existieren unterschiedliche Kategorien für das Off-Chaining: Verifizierende Berechnung (Zero Knowledge Proofs), Enklaven, Secure-Multiparty-Computation (sMPC), Anreizsysteme.

Verifizierende Berechnung Mit Hilfe von Beweisen (Zero-Knowledge-Proofs – ZKPs) kann mathematisch sicher nachgewiesen werden, dass eine Datengrundlage oder Berechnung vorab festgelegte Restriktionen oder Attribute erfüllt, ohne die Ausgangswerte enthüllen zu müssen.

Enklaven Innerhalb eines physisch abgeschirmten Bereiches eines Prozessors können Berechnungen in sicheren Entwicklungsumgebungen (Trusted Execution Environments – TEEs) ausgeführt werden. Der Vorteil dieser Umgebungen ist, dass softwareseitig keine Angriffsvektoren existieren.

Secure Multiparty Computation (sMPC) Der Rechenaufwand wird auf mehrere Instanzen aufgeteilt, um einen „Single-Point-Of-Failure“ und „Single-Point-Of-Truth“ zu vermeiden. Entscheidend ist hierbei, dass keine einzelne Instanz Zugriff

auf die Datengrundlage erhält. Berechnungen von Statusänderungen müssen öffentlich auditierbar sein, um das Risiko einer Kompromittierung zu minimieren.

Anreiz-basiertes Off-Chaining Mit Hilfe von Anreizmechanismen werden Teilnehmer dazu motiviert eine korrekte Berechnung durchzuführen bzw. sich nicht schädliche zu verhalten. Grundlage ist die Annahme eines rationalen ökonomisch motivierten Verhaltens. Auch hier müssen Berechnungen öffentlich auditierbar sein, damit definierte Mechanismen des Systems durchgesetzt werden können.

5 Lösungsbeschreibung

Auf Basis der Anforderungen und unter Verwendung der Designprinzipien können technische Spezifikationen der Zielarchitektur (vgl. Abb. 1) abgeleitet werden. Die Infrastruktur setzt sich aus drei verschiedenen Netzwerken zusammen, welche unterschiedliche Funktionen für die Anwendung erfüllen. Mit Hilfe von Off-Chaining Technologien lässt sich ein Protokoll für das Validierungsnetzwerk implementieren, welches Daten mit hohen Sicherheitsanforderungen abseits des öffentlichen Blockchain-Netzwerkes vertrauensvoll validiert. Eine kryptografisch geschützte Datenübertragung sichert den Datenaustausch zwischen Parteien und Netzwerken. Dokumentreferenzen und Validitätsnachweise werden über Smart Contracts auf der Blockchain aggregiert und gespeichert. Im Folgenden sind Netzwerk-Spezifikationen der Zielarchitektur sowie Merkmale der Datenübertragung und der Smart Contracts erläutert.

Blockchain-Netzwerk Das Netzwerk verfügt über eine Ethereum Virtual Machine (EVM). Die Wahl der EVM ist durch den Grad der technischen Ausgereiftheit, die Verfügbarkeit weiterführender Frameworks sowie das größte Potenzial für einen langfristigen technischen Support begründet. Die EVM ermöglicht außerdem die Ausführung von Smart-Contracts, um Prozesslogik auf der Blockchain abzubilden, Bauteil und Dokumenten-Hierarchien zu implementieren sowie Zugriffs- und Eigentumsrechte zu vergeben.

Eine öffentliche Netzwerkkonfiguration ist bevorzugt, um eine persistente Datenhaltung und hohe Datenintegrität zu realisieren. Da es bei starker Netzwerkauslastung zu Engpässen in der Datenspeicherung und somit zu erhöhten Nutzungskosten

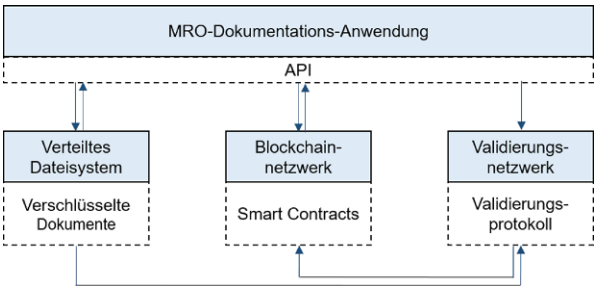

Abb. 1 Zielarchitektur-Datenfluss schematisch

kommen kann, werden nur ausgewählte Metadaten in der Blockchain abgelegt. Um dennoch eine persistente Datenspeicherung für sämtliche Dokumente zu ermöglichen, ist die Anwendung um ein verteiltes Dateisystem erweitert.

Verteiltes Dateisystem Das Dateisystem speichert sämtliche MRO-Dokumente. Ähnlich einem Blockchain-Netzwerk, werden Daten über viele Knoten repliziert und synchronisiert. Zudem verfügt das Netzwerk über eine Versionskontrolle, sodass Änderungen leicht detektierbar sind. Im Gegensatz zu einer Blockchain, erweist es sich als deutlich (kosten)effizienter bei der Datenspeicherung, da es über keine Virtual Machine und keinen Konsensfindungsmechanismus verfügt.

Validierungsnetzwerk Das Validierungsnetzwerk führt ein Protokoll aus und vereint dabei verschiedene Off-Chaining Technologien, um eine vertrauensvolle Validierung abseits des öffentlichen Blockchain-Netzwerkes durchzuführen. Unter Verwendung eines sMPC-Ansatzes sind mehrere unabhängige Knoten zusammengeschlossen, die gemeinsam die technische Überprüfung der MRO-Dokumentationen ausführen und die Validität für sämtliche Anwender prüfen. Dabei haben einzelne Knoten keinen Zugriff auf Dokumente. Erst durch gemeinsame Koordinierung der Knoten kann die Validitätsprüfung vollzogen werden. Dieser Gemeinschaftsaufwand minimiert folgende Risiken: Ausfall des Systems („Single-Point-Of-Failure"), Kompromittierung, Datenmissbrauch.

Ein eigens für den Anwendungsfall entwickeltes Validierungsprotokoll implementiert die zugrundeliegende Funktionsweise auf allen Knoten des Netzwerkes (vgl. Abb. 2). Die Entschlüsselung und algorithmische Überprüfung der Dokumente findet in einer Enklave, in Form eines Trusted Execution Environment (TEE), statt. Eine Entschlüsselung und Überprüfung sensitiver MRO-Dokumente ist möglich, ohne das unautorisierte Zugriffsmöglichkeiten bestehen. Unter Verwendung einer verifi-

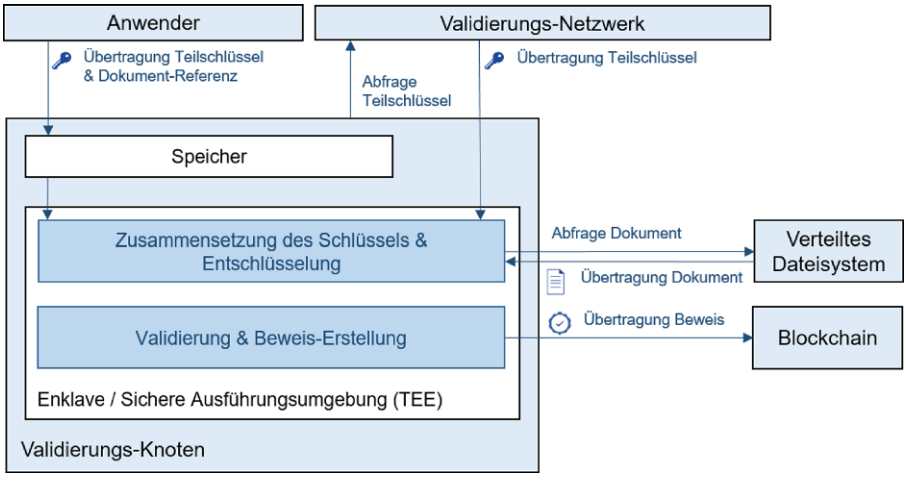

Abb. 2 Validierungsprotokoll schematisch

zierenden Berechnung sind Validitätsprüfungen als Zero-Knowledge-Proofs auf der Blockchain dokumentiert.

Datenübertragung & Verschlüsselung Generell sind alle MRO-Dokumente im Dateisystem verschlüsselt. Damit Dokumente von Anwender zu Anwender oder von Anwender zu Validierungsnetzwerk zugänglich sind, erfolgt ein verschlüsselter Austausch von Passwörtern. Hierbei kommen zwei verschiedene Verschlüsselungsverfahren zum Einsatz. Die Übertragung von Passwörtern auf der Blockchain ist über eine asymmetrisches Kryptosystem realisiert. Bei der Peer-to-Peer Weiterleitung der Passwörter an das Validierungsnetzwerk kommt zusätzlich ein Schwellwertverfahren zum Einsatz. Bei diesem Verfahren erhält jeder Knoten des Validierungsnetzwerkes einen Teilschlüssel. Die Festlegung eines Schwellwertes bestimmt die Anzahl der Knoten die kollaborieren müssen, um aus den Teilschlüsseln das zuvor aufgeteilte Passwort wiederherstellen zu können. Erst nach Wiederherstellung des Passwortes kann innerhalb einer Enklave ein Dokument entschlüsselt und validiert werden.

Smart Contracts Die Geschäfts-/Prozesslogik ist auf der Blockchain mittels Smart Contracts abgebildet. Um eine Bauteil-Dokumenten-Historie und die Zugehörigkeit zu bestimmten Bauteilen zu definieren, sind sogenannten non-fungible-tokens (NFTs) implementiert. Analog zu der Einzigartigkeit von physischen Flugzeugersatzteilen bzw. Bauteilen können diese digitalen Einheiten anhand eines Hash-Wertes eindeutig identifiziert werden. In Hinblick auf die MRO-Dokumentationen lassen sich Verantwortlichkeiten oder Besitzverhältnisse festlegen und für das gesamte Netzwerk darstellen. Den Dokumenten zugehörige Attribute lassen weitere Informationen erkennen, wie zum Beispiel den Status der Validierung.

6 Ausgangswissen – Diskussion und praktische Implikationen

Interaktionen der Anwender mit dem System zeigen die Funktionalität des Netzwerkes und wie technische Spezifikationen zur Anforderungserfüllung beitragen. Im Folgenden sind die Interaktionen „Flugzeugersatzteil registrieren, Zertifikat-Upload und Zertifikat-Validierung“ beispielhaft dargestellt (vgl. Abb. 3).

Flugzeugersatzteil registrieren (1): Ein Anwender erstellt ein Flugzeugersatzteil im System. – Systemoperationen: Es wird eine Bauteil-Dokumenten-Hierarchie auf der Blockchain initialisiert.

Zertifikat-Upload (2): Ein Anwender lädt ein Dokument in das System. – Systemoperationen: Das Dokument wird verschlüsselt, im verteilten Dateisystem abgelegt und bekommt eine eindeutige Adresse, die fortan als Referenz dient. Die Adresse des Dokumentes wird in entsprechender Bauteil-Dokumenten-Hierarchie auf der Blockchain gespeichert.

Zertifikat-Validierung 1 (3): Ein Anwender erbittet die Validierung eines Dokuments. – Systemoperationen: Der Schlüssel wird in Teilschlüssel aufgeteilt und

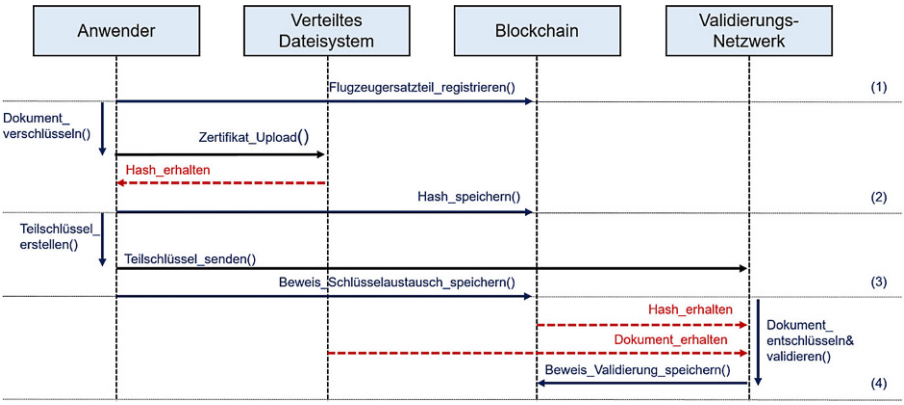

Abb. 3 Sequenzdiagram – Flugzeugersatzteil registrieren, Zertifikat-Upload und Zertifikat-Validierung

ein Schwellwert festgelegt, basierend auf der Anzahl der Knoten die im Validierungsnetzwerk zur Verfügung stehen. Die Teilschlüssel werden samt Dokument-Referenz an die Knoten des Validierungs-Netzwerkes gesendet. Weiterhin wird auf der Blockchain ein Beweis gespeichert, dass die Teilschlüssel zur Validierung versendet wurden.

Zertifikat-Validierung 2 (4): Das Validierungsnetzwerk validiert automatisch erhaltene Dokument-Referenzen. – Systemoperationen: Für erhaltene Dokument-Referenzen werden Teilschlüssel von Validierungsknoten abgefragt. Beim Erreichen des Schwellwertes wird der Schlüssel innerhalb einer sicheren Ausführungsumgebung (TEE) wiederhergestellt und Dokumente zur Validierung entschlüsselt. Geprüft wird auf formale Richtigkeit und Cross-Referenzen. Werden alle Kriterien gemäß dem Algorithmus erfüllt, wird ein Beweis auf die Blockchain geschrieben, dass das Dokument geprüft und valide ist.

Eine persistente Datenhaltung ist erreicht, da MRO-Dokumente im verteilten Dateisystem dauerhaft zur Verfügung stehen. Metadaten der Dokumente sowie Systemoperationen und Validitäts-Nachweise sind auf der öffentlichen Blockchain dauerhaft gespeichert. Trotz Synchronisierung der Daten im Netzwerk kann die Privatsphäre gewahrt bleiben, da MRO-Dokumente verschlüsselt sind. Zudem erfolgt die Entschlüsselung der Dokumente nicht durch eine zentrale Instanz, sondern durch ein Netzwerk an Validierungsknoten innerhalb einer physisch abgeschirmten Enklave. Da Anwender stets alleinige Verwalter ihrer generierten Passwörter sind, obliegt ihnen auch die selektive Weitergabe. Einzelne Validierungsknoten verfügen lediglich über Teilschlüssel und besitzen somit keine Zugriffsmöglichkeit. Dokumente die eine Validierung benötigen, können innerhalb der Enklaven geprüft werden. Durch die Durchführung von verifizierenden Berechnungen und die Speicherung der Beweise auf der Blockchain, in Form von Zero-Knowledge-Proofs, kann die Validität von MRO-Dokumenten gegenüber anderen Netzwerkteilnehmern bestätigt werden. Die Zuweisung von Dokumenten, Metadaten (zum Beispiel Eigentum, Verantwortlich-

keiten u. a.) und Beweisen innerhalb einer Token gestützten Bauteil-Dokumenten-Hierarchie, ermöglicht eine digitale Abbildung der MRO-Dokumentationsprozesse.

Die vorgestellte Architektur beschreibt die Infrastruktur einer Blockchain-basierten Plattformlösung für Dokumentationsprozesse der MRO-Branche. An den Beispiel-Interaktionen zeigt sich, dass anfangs beschriebene Anforderungen erfüllt werden können. In Hinblick auf die Ziele von RAPADO kann die Lösung zur verschlüsselten und validierten Ablage von Dokumenten beitragen. Funktionalitäten zur Authentifizierung von autorisierten Anwendern sind nicht beschrieben und stellen eine Erweiterung der Ergebnisse in zukünftigen Untersuchungen dar. Das Konzept ist generisch gehalten und ließe sich auf verwandte Anwendungsfälle und Branchen übertragen. Insbesondere die Einbeziehung der Off-Chaining Konzepte kann beschriebene Designprinzipien erweitern und zur Konfliklösung im Designprozess beitragen. Dabei wird insbesondere eine Möglichkeit aufgezeigt, wie Privatsphäre in einem öffentlichen Blockchain-Netzwerk gewahrt bleiben kann. Für den konkreten Fall bleibt zu klären, welches öffentliche Netzwerk am besten geeignet ist. Dabei steht die Frage der Skalierbarkeit hinsichtlich Kosten und Performanz im Fokus. Zudem muss die Zuverlässigkeit des Validierungsmechanismus eingehend geprüft werden. Engpässe könnten durch eine hohe Rechenintensität bei der der Generierung von Beweisen entstehen. Die Erprobung der Architektur durch MRO-Experten ermöglicht eine qualitative Evaluation der Ergebnisse des DSR-Projektes (Hevner et al. 2004). Unter realen Bedingungen steht die Bewährung aus.

Danksagung Dieser Beitrag ist Teil des Forschungsprojektes „RAPADO“. Ziel des Verbundprojektes ist die Schaffung eines Rahmenwerkes und einer Plattform für die authentifizierte, verschlüsselte und validierte Ablage von Dokumentationen von Flugzeugersatzteilen zur Standardisierung durch die Aufsichtsbehörden. Verbundpartner aus der Industrie ist die Opremic trade GmbH. Das Projekt ist vom Bundesministerium für Wirtschaft und Klima der Bundesrepublik Deutschland im Rahmen des Luftfahrtforschungsprogramms LuFo VI-1 gefördert. Wir bedanken uns bei den Experten, unserem Partner und bei dem Förderer für die Unterstützung.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Aleshi A, Seker R, Babiceanu RF (2019) Blockchain model for enhancing aircraft maintenance records security. IEEE International Symposium on Technologies for Homeland Security (HST), pp 1–7. https://doi.org/10.1109/HST47167.2019.9032943

Barak B, Goldreich O, Impagliazzo R, Rudich S, Sahai A, Vadhan S, Yang K (2012) On the (im)possibility of obfuscating programs. J ACM 59(2):1–48. https://doi.org/10.1145/2160158.2160159

vom Brocke J, Maedche A (2019) The DSR grid: six core dimensions for effectively planning and communicating design science research projects. Elect Markets 29:379–385. https://doi.org/10.1007/s12525-019-00358-7

Buterin V (2015) On public and private blockchains. Ethereum Foudation Blog. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Zugegriffen: 05.05.2022

Buterin V (2016) Privacy on the blockchain. Ethereum Foudation Blog. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. Zugegriffen: 05.05.2022

Eberhardt J, Heiss J (2018) Off-chaining models and approaches to off-chain computations. In Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, SERIAL 2018, pp 7–12. Association for Computing Machinery, New York. https://doi.org/10.1145/3284764.3284766

Efthymiou M, McCarthy K, Markou C, O'Connell JF (2022) An exploratory research on blockchain in aviation: the case of maintenance, repair and overhaul (MRO) organizations. Sustainability 14:2643. https://doi.org/10.3390/su14052643

Garg S, Gentry C, Halevi S, Raykova M, Sahai A, Waters B (2013) Candidate indistinguishability obfuscation and functional encryption for all circuits. In 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS), pp 40–49. Berkeley, CA, USA. https://doi.org/10.1109/FOCS.2013.13

Gleasure R (2013) What is a 'wicked problem' for IS research? In Proceedings of the 2nd international SIG Prag workshop on "IT Artefact Design & Workpractice Improvement". http://www.vits.org/adwi2013/RGleasure-ADWI2013.pdf. Zugegriffen: 19.07.2022

Hasan HR, Salah K, Jayaraman R, Ahmad RW, Yaqoob I, Omar M (2020) Blockchain-based solution for the traceability of spare parts in manufacturing. In IEEE Access 8, pp 100308–100322. https://doi.org/10.1109/ACCESS.2020.2998159

Hevner A, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Quart 28(1):75–105. https://doi.org/10.2307/25148625

Holbrook J (2020) Architecting enterprise blockchain solutions. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119557722

Lohmer J, Lasch R (2020) Blockchain in operations management and manufacturing: Potential and barriers. Comp Ind Eng. https://doi.org/10.1016/j.cie.2020.106789

Manjunath P, Herrmann M, Sen H (2019) Implementation of blockchain data obfuscation. In Chen YW, Zimmermann A, Howlett R, Jain L (eds) Innovation in Medicine and Healthcare Systems, and Multimedia. Smart Innovation, Systems and Technologies, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-13-8566-7_49

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Zugegriffen: 05.05.2022

Schyga J, Hinckeldeyn J, Kreutzfeldt J (2019) Prototype for a permissioned blockchain in aircraft MRO. In Proceedings of the Hamburg International Conference of Logistics (HICL) 2019 (27). Epubli GmbH. https://doi.org/10.15480/882.2480

Venable JR (2006) The role of theory and theorising in design science research. In Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESRIST) Claremont, CA (CGU), pp 1–18

Wickboldt C, Kliewer N (2018) Blockchain zur dezentralen Dokumentation von Werkstattereignissen in der Luftfahrtindustrie. HMD 55(6):1297–1310. https://doi.org/10.1365/s40702-018-00452-y

Wickboldt C, Kliewer N (2019) Blockchain for workshop event certificates – a proof of concept in the aviation industry. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, June 8–14, 2019

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com