November 2022

DIN SPEC 32790

ICS 35.240.99

Referenzarchitektur für Blockchain-Applikationen zur Schaffung von Transparenz in Supply-Chains

Reference architecture for blockchain applications to create transparency in supply chains

Architecture de référence pour les applications blockchain afin de créer de la transparence dans les chaînes d'approvisionnement

Gesamtumfang 30 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

www.din.de
www.beuth.de

Alleinverkauf durch Beuth Verlag GmbH, 10772 Berlin

3385071

Inhalt

Bilder

Tabellen

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in DIN-SPEC-Konsortien und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Die vorliegende DIN SPEC ging aus dem Projekt „ABChain“ hervor. Das IGF-Vorhaben 21256 N der Forschungsvereinigung FIR e. V. an der RWTH Aachen wird über die AiF im Rahmen des Programms zur Förderung der industriellen Gemeinschaftsforschung (IGF) vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) aufgrund eines Beschlusses des Deutschen Bundestages gefördert.

Die Erarbeitung und Verabschiedung des Dokuments erfolgten durch die nachfolgend genannten Initiator(en) und Verfasser:

Initiator

— FIR e.V. an der RWTH Aachen

  Jessica Rahn

Verfasser

— CircularTree GmbH

  Kathrin Adam

— GS1 Germany GmbH

  Tim Bartram

— Dr. Babor GmbH & Co. KG

  Rupert Freutsmiedl

— Advanced-Materials-Concepts GmbH

  Achim Hofmann, Sabine Köller

— HolyPoly GmbH

  Gunter Miegel

— IOTA Foundation

  Eicke Schütze

— Westa-Holding GmbH & Co. KG (Westaflex)

  Jan Westerbarkey

Für dieses Thema bestehen derzeit keine Normen im Deutschen Normenwerk.

DIN SPEC sind nicht Teil des Deutschen Normenwerks.

Für diese DIN SPEC wurde ein Entwurf veröffentlicht.

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann das DIN-SPEC-Konsortium weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass das DIN-SPEC-Konsortium für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die kostenfreie Bereitstellung dieses Dokuments als PDF-Version über den Beuth WebShop wurde im Vorfeld finanziert.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Einleitung

Mit dem Zuwachs an Bedeutung in der Gesellschaft sind auch für Unternehmen Nachhaltigkeitsaspekte wichtiger geworden [1]. Dazu zählen Kriterien wie der Energieverbrauch, CO_2-Ausstoß oder die soziale Verantwortung gegenüber Mitarbeitenden des eigenen Betriebs und von Zulieferern [2]. Um Aussagen über Endprodukte treffen zu können, müssten die entsprechenden Informationen über die gesamte Lieferkette aufgenommen und verteilt werden, was nur mit Hilfe von Transparenz umgesetzt werden kann [1].

Die Sichtbarkeit von Produkt- und Bewegungsdaten im gesamten Netzwerk, d. h. über die eigenen Unternehmensgrenzen hinaus, ist auch eine Grundvoraussetzung für eine effiziente Wertschöpfungskette. Aufgrund von sinkender Wertschöpfungstiefe der einzelnen Unternehmen findet die Wertschöpfung mit einer zunehmenden Anzahl an Partnern in Wertschöpfungsnetzwerken statt. Um in diesen undurchsichtiger und komplexer werdenden Wertschöpfungsstrukturen die Beherrschbarkeit zu bewahren, sollten sich Unternehmen in der Supply-Chain miteinander vernetzen [3] [4].

Mit der stärkeren Verflechtung der Unternehmen und dem Austausch umfassender, teilweise sensibler Daten, gewinnen auch die Themen Datensicherheit und Datenschutz an Relevanz [5]. Die zunehmende Integration von IT-Systemen erhöht ebenfalls den potenziellen Schaden durch Angriffe, sodass auf der IT-Sicherheit, vor allem bei einer überbetrieblichen Systemintegration, ein starker Fokus liegen sollte [6].

Aus diesen zentralen Problemstellungen lassen sich Anforderungen an eine Supply-Chain-übergreifende Dateninfrastruktur für kleine- und mittlere Unternehmen (KMU) formulieren. Eine solche Dateninfrastruktur sollte:

— die Sichtbarkeit von Produkt- und Nachhaltigkeitsdaten im gesamten Wertschöpfungsnetzwerk ermöglichen;

— eine Grundlage für ein dezentrales Supply-Chain-Management schaffen;

— Datensicherheit sicherstellen.

Auf der technologischen Seite können diese Anforderungen durch eine Blockchain-Applikation, als verteilte und fälschungssichere Datenbank erfüllt werden. Die Eigenschaften einer Blockchain schließen es aus, dass abgelegte Daten unter vertretbarem Aufwand unbemerkt manipuliert oder gelöscht werden können. Gleichzeitig wird ein einfacher überbetrieblicher Zugriff auf die Informationen sichergestellt. Blockchains basieren auf kryptografischen Hashfunktionen, welche die Informationen in eine Zeichenfolge fixer Länge umwandeln, den Hashwert. Dabei ergeben dieselben Informationen immer denselben Hashwert, auch nur leicht veränderte Funktionen ergeben jedoch einen stark abweichenden Hashwert, während der Hashwert selbst keine Informationen preisgibt [7] [8]. Die Echtheit der Information kann zudem durch eine Verschlüsselung sichergestellt werden. Dabei kann beispielsweise eine asymmetrische Verschlüsselung genutzt werden, bei der mit Hilfe eines zueinander passenden Schlüsselpaars Versender und Empfänger verifiziert werden [7]. Mit Hilfe dieser beiden Mechanismen kann eine Manipulation von Informationen nicht unentdeckt erfolgen und die Integrität der Informationen sichergestellt werden. Die Sicherheit gegen den Datenverlust wird durch die dezentrale Speicherung bei einer ausreichenden Anzahl an Netzknoten sichergestellt [9]. Das bedeutet, dass bei dem Verlust von Daten in einem Unternehmen, bzw. an einem Netzknoten, die Daten noch bei anderen Teilnehmenden der Blockchain (Stakeholder) gesichert sind. Das Risiko für einen permanenten Verlust von Daten ist somit minimal. Diese dezentrale Speicherung führt auch dazu, dass alle Teilnehmenden die Daten lokal zur Verfügung haben und somit jederzeit darauf zugreifen können.

Um die Implementierung einer solchen Lösung zu vereinfachen, bietet dieses Dokument einen Leitfaden für die Gestaltungsmöglichkeiten einer Blockchain-Applikation, indem die Vor- und Nachteile der einzelnen Lösungsbausteine dargelegt und diskutiert werden, sodass Unternehmen die für sie passende Lösung einfacher auswählen können.

1 Anwendungsbereich

Dieses Dokument legt einen Gestaltungsleitfaden zur technischen Ausgestaltung von Blockchain-Applikationen für verschiedene Anwendungsfälle im Supply-Chain-Management fest. Dies umfasst auch die Festlegung von erforderlichen Daten und Informationen, die die Teilnehmenden bereitstellen müssen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN SPEC 16597, *Terminologie für Blockchains; Text Englisch*

DIN EN ISO 22739[1], *Blockchain und Technologien für verteilte elektronische Journale — Vokabular*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach DIN SPEC 16597 und DIN EN ISO 22739.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— DIN-TERMinologieportal: verfügbar unter https://www.din.de/go/din-term

— DKE-IEV: verfügbar unter https://www.dke.de/DKE-IEV

4 Inhaltliche Einführung

4.1 Blockchain

Eine Blockchain ist eine Form der Distributed Ledger Technology (DLT), die primär eine Technologie zur dezentralen Speicherung von Transaktionen darstellt. Um dies besonders verlust- und manipulationssicher zu gestalten, und gleichzeitig eine hohe Verfügbarkeit der Daten sicherzustellen, greift die DLT auf verschiedene technologische Lösungsbausteine zurück.

Blockchains, und damit DLTs, basieren auf kryptografischen Hashfunktionen, welche Informationen in eine Zeichenfolge fixer Länge umwandeln, den Hashwert. Dabei ergeben dieselben Informationen immer denselben Hashwert, während auch nur leicht veränderte Informationen jedoch einen stark abweichenden Hashwert erzeugen. Dabei gibt der Hashwert selbst keine Informationen preis [7] [8]. Die Echtheit der Information wird zudem durch ein mathematisches Schlüsselpaar sichergestellt. Der Versender der Information signiert mit seinem persönlichen Schlüssel, während der Empfänger die Daten nun mit dem zum Versender passenden Schüssel öffnen kann [7]. Mit Hilfe dieser beiden Mechanismen kann eine Manipulation von Informationen nicht unentdeckt erfolgen und die Integrität der Informationen sichergestellt werden. Die Sicherheit gegen den Datenverlust wird bei einer ausreichenden Anzahl an Netzknoten durch die dezentrale Speicherung sichergestellt [9]. Das bedeutet, dass bei dem Verlust von Daten in einem Unternehmen, bzw. an einem Netzknoten, die Daten noch bei anderen Stakeholdern gesichert sind. Das Risiko eines dauerhaften Verlusts von Daten ist somit minimal. Diese dezentrale Speicherung führt auch dazu, dass alle beteiligten Stakeholder die Daten lokal zur Verfügung haben und somit jederzeit darauf zugreifen können.

In einer Blockchain können sogenannte Smart Contracts verwendet werden, das sind Verträge (nicht im Juristischen Sinn), die in Form eines Computerprogramms in der Blockchain hinterlegt sind (ISO 22739:2020,

1 Aktuell noch im Entwurf. Referenzfassung bereits in Englisch erschienen als ISO 22739:2020 [10].

3.72 [10]). Der Nutzen kann über viele Anwendungsbereiche hinweg variieren (z. B. Zahlungsausschüttung bei Wareneingang).

Die wesentlichen Vorteile einer Blockchain lassen sich nur durch möglichst viele aktive Partner der Supply-Chain nutzen. Die Möglichkeit, in einem Konsortium zusammenzuarbeiten, ohne dass eine zentrale Vertrauenseinheit benötigt wird, ist somit ein wesentlicher intrinsischer Anreiz zur Teilnahme an einer Blockchain-Applikation. Darüber hinaus gibt es weitere Anreizmöglichkeiten, die von handelbaren Coins und somit monetären Belohnungen, über rein intrinsische, außerwirtschaftliche Motivation bis hin zu bindenden vertraglichen Regelung reichen.

Wenn in diesem Themenkomplex von Transaktionen gesprochen wird, ist nicht nur die aus den Wirtschaftswissenschaften bekannte (ökonomische) Transaktion gemeint, bei der ein Wirtschaftsobjekt von einem Wirtschaftssubjekt zum anderen übergeht. Im Folgenden ist der Begriff „Transaktion" als ein Ereignis (Event) in der Wertschöpfungskette zu verstehen, durch den ein neuer konsistenter und definierter Datensatz erzeugt wird [11].

4.2 Dezentrale digitale Identifikatoren – Decentralized Identifiers (DIDs)

Für eine transparente Supply-Chain ist eine eindeutige, sichere Identifizierung des Urhebers jeder Nachricht in einer „trustless" Form wichtig, ohne dass dazu einer zentralen Instanz vertraut werden muss. Eine DID speichert eine Liste von Eigenschaften zu einer Identität und bietet die Möglichkeit, diese selektiv nachzuweisen. Dazu wird für jede DID ein Schlüsselpaar erzeugt, das prinzipiell dezentrale Anwendungsfälle zulässt, die eine Public-Key-Infrastruktur (PKI) mit zentraler Autorität bietet.

Das Konzept der Self Souvereign Identity (SSI) erlaubt es, jeweils nur den benötigten Teil der Identität preiszugeben, der im konkreten Fall benötigt wird. So kann Transparenz erzeugt werden, ohne an anderer Stelle den Datenschutz zu vernachlässigen. Beispielsweise kann ein Altersnachweis erfolgen, ohne den Geburtsort oder das Geburtsdatum preiszugeben.

DIDs bieten die Möglichkeit, mit Verifiable Credentials (VC) flexible Zertifikate für ausgewählte Merkmale einer DID zu erstellen. Die VC können off-chain, außerhalb einer Blockchain-Applikation, (ISO 22739:2020, 3.52 [10]) übertragen und on-chain, innerhalb einer Blockchain-Applikation, (ISO 22739:2020, 3.54 [10]) verifiziert werden. Beispielsweise können vertrauenswürdige Geschäftspartner ihren Mitarbeitenden VC erstellen, die sie individuell für den Zugriff auf eine bestimmte Warengruppe bevollmächtigen. Dabei überträgt sich das Vertrauen gegenüber einem Verifizierer beim Ausstellen des Zertifikats auf den Besitzer.

DIDs sind Identifikatoren, die eine überprüfbare, dezentrale digitale Identität ermöglichen. Eine DID bezieht sich auf ein beliebiges Subjekt (z. B. eine Person, Organisation, Sache, ein Datenmodell, eine abstrakte Entität usw.). DIDs können von einem oder mehreren DID-Controllern erstellt und verwaltet werden [12].

Im Gegensatz zu typischen föderierten Identifikatoren wurden DIDs so konzipiert, dass sie unabhängig von zentralisierten Registern, Identitätsanbietern und Zertifizierungsstellen verwendet werden können. DIDs ermöglichen durch ihr spezifisches Design die Überprüfung einer DID durch Dritte, ohne die Erlaubnis des Herausgebers dafür zu benötigen. DIDs sind Uniform Resource Identifier (URI), die ein DID-Subjekt mit einem DID-Dokument verknüpfen, was vertrauenswürdige Interaktionen ermöglicht, die diesem Subjekt zugeordnet sind.

Jedes DID-Dokument kann kryptografisches Material, Verifizierungsmethoden oder Dienste ausdrücken, die eine Reihe von Mechanismen bereitstellen, die es einem DID-Controller ermöglichen, die Kontrolle über die DID nachzuweisen. Dienste ermöglichen vertrauenswürdige Interaktionen, die dem DID-Subjekt zugeordnet sind. Eine DID kann die Mittel bereitstellen, um das DID-Subjekt selbst zurückzugeben, wenn das DID-Subjekt eine Informationsressource wie beispielsweise ein Datenmodell ist [12].

4.3 Anforderungen an Blockchain-Applikationen in Supply-Chains

Die hier aufgeführten Anforderungen wurden im Rahmen des Forschungsprojekts ABChain erarbeitet. Innerhalb dieses Forschungsprojekts wurde auch die Erstellung dieses Dokuments initiiert.

Eine zentrale Anforderung durch alle Anwender, wie auch in Bild 1 dargestellt, war die nahtlose Integration einer Blockchain Lösung in bestehende IT-Systeme, um den Aufwand im Tagesgeschäft zu minimieren. Hierbei sollte stets die Möglichkeit zur Unterscheidung zwischen relevanten und irrelevanten Daten für das Teilen entlang der Lieferkette gegeben werden. Bei der Synchronisierung der Daten sollte außerdem eine Konsistenzprüfung erfolgen, die das Schreiben falscher Informationen in die Blockchain erschwert. Eine große Rolle spielte auch die Datensicherheit und der Zugriff auf die Daten durch Partner sowie Dritte. Dabei waren vor allem die Erstellung eines Informationssicherheitskonzeptes und das Einhalten der DSGVO [16], also auch das Löschen von Daten zu ermöglichen, zentrale Anforderungen. Außerdem war es den Anwendern aus produzierenden Unternehmen sehr wichtig, dass sie selbst bestimmen können, wer welche Daten einsehen kann. Die Steuerung, welche Daten auch im späteren Verlauf der Lieferkette an Dritte oder die Öffentlichkeit gelangen können, sollte sehr präzise ermöglicht werden. Bei den Logistikdienstleistern war dies kein Fokus, da größtenteils durch deren Kunden gesteuert wird, wer die Daten einsehen kann und die Datenhoheit nicht bei ihnen selbst liegt. Diese Sicherheitsanforderungen können technologisch über die Schlüsselpaare in der Blockchain sowie die redundante Datenhaltung erfüllt werden. Im Rahmen der Gestaltung der Zugriffsrechte war auch die Governance der Blockchain-Applikation ein wichtiges Thema. Hierbei gilt es, diejenigen Unternehmen und Richtlinien zu bestimmen die im Zweifelsfall über die Gültigkeit von Daten und Transaktionen entscheiden können.

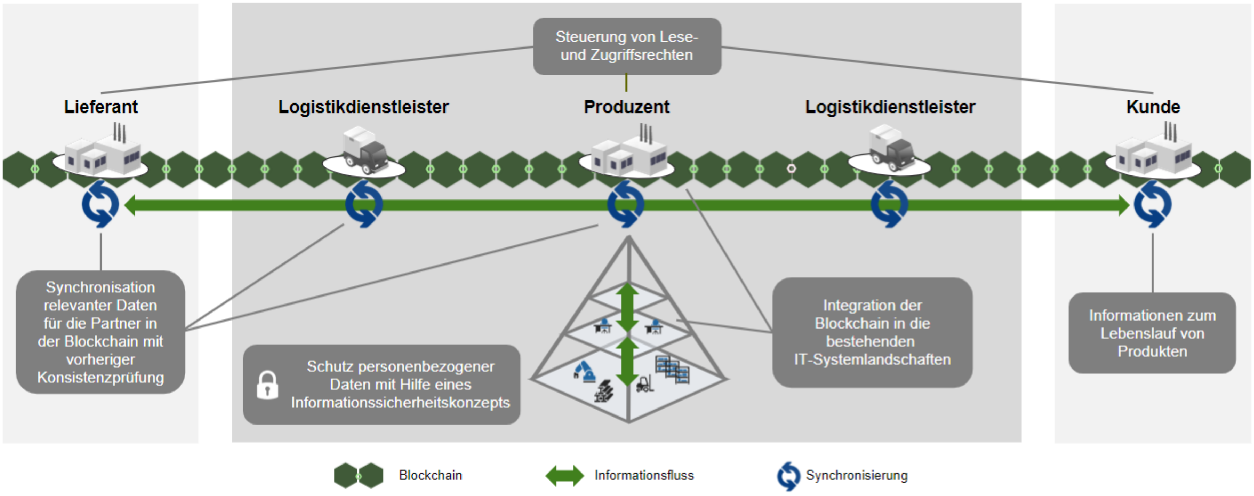

Bild 1 — Integration von Blockchain-Technologie in bestehende IT-Systeme

Für Blockchain-Applikationen in der Supply-Chain ist die Lastenheftvorlage in Anhang A anzuwenden.

4.4 Anwendungsfälle

Zur Identifikation relevanter Anwendungsfälle wurden im Forschungsprojekt ABChain Interviews mit potenziellen Anwendenden in Unternehmen durchgeführt.

Zu den wichtigsten Anwendungsfällen der interviewten Personen zählen eine allgemeine Produktrückverfolgung über den Lebenslauf des Produkts und insbesondere von Nachhaltigkeitskriterien wie dem CO_2-Verbrauch entlang der ganzen Lieferkette. Auch die Rückverfolgung von Zertifikaten ist als Anwendungsfall herausgestellt worden, da diese insbesondere bei Bio- oder fair hergestellten Rohstoffen bzw. Produkten eine große Rolle spielt. Neben den Anwendungsfällen im Bereich der Nachhaltigkeit wurde außerdem die Abwicklung von Zahlungen bei Lieferungen, insbesondere bei Schüttgut oder aber eine Rückverfolgung sicherheitsrelevanter Bauteile von Produkten aufgeworfen. Die generelle Transparenz in der Supply-Chain, die durch die Einführung einer solchen Lösung geschaffen wird, ermöglicht jedoch noch viele weitere Anwendungsfälle zur Optimierung und Verbesserung der überbetrieblichen Prozesse.

Beispielhaft werden in Anhang B unterschiedliche Anwendungsfälle aus der Praxis dargestellt:

Abschnitt B.1	CO_2-Fußabdruck;
Abschnitt B.2	Rückverfolgung von Lebensmitteln;
Abschnitt B.3	Lieferkette Luft- und Raumfahrt und Automobilindustrie;
Abschnitt B.4	Konfliktrohstoffe;
Abschnitt B.5	Papierlose Zollabfertigung;
Abschnitt B.6	Zertifiziertes Kunststoffrezyklat.

4.5 Technische Grenzen — das Orakelproblem

Bevor Daten von außerhalb in die Blockchain einbezogen werden, muss deren Richtigkeit, Authentizität und Integrität abgesichert sein. Diese Absicherung ist nur im begrenztem Maße durch technische Maßnahmen möglich und bedarf letztendlich organisatorischer Lösungen. Organisatorische Lösungen bedingen, dass sich die teilnehmenden Parteien vertrauen. Diese Problemstellung wird als „Blockchain Oracle Problem“ beschrieben (siehe Caldarelli [13]) und markiert die Grenze der technisch nicht lösbaren Anwendungsfälle für die Verwendung von Blockchain-Technologie für das Supply-Chain-Management.

Ein Beispiel sind Temperatursensoren, die die Schwankungen ihrer Umgebung melden, aber letztendlich nicht sicherstellen können, dass diese auch für die transportierten Güter gelten.

Einen Ansatz zur Mitigation des Oracle Problems liefert ein Scoring der Vertrauenswürdigkeit von Daten. Dabei wird das Risiko abgeschätzt, dass die Daten auf dem Weg vom Sensor zur nutzenden Applikation verändert wurden. Ein Beispiel dafür ist das Software Development Kit (SDK) aus dem Project Alvarium [14]. Dies löst zwar den technischen Teil (Datenveränderung) des Oracle Problems, nicht aber eine Beeinflussung außerhalb des Sensors.

5 Referenzarchitektur — Taxonomie einer Blockchain-Applikation

5.1 Allgemeines

Die Blockchain Technologie, oder auch DLTs im Gesamten, können durch ihre breiten Variationen in verschiedensten Themenfeldern genutzt werden. Blockchain basierte Systeme und Applikationen unterliegen dadurch der Schwierigkeit, dass sich in der Entwicklung zwischen einer Vielzahl an Konfigurationen entschieden werden muss. Im Folgenden wird ein Überblick über die im Supply-Chain-Management verwendeten und bei der Erarbeitung dieser DIN SPEC identifizierten Merkmale und ihrer möglichen Ausprägungen gegeben, sodass sich im Gesamten eine Taxonomie der Blockchain-Applikation ergibt, die in Tabelle 1 dargestellt ist.

Tabelle 1 — Taxonomie einer Blockchain-Applikation

Merkmal	Ausprägungen					
Grad der Datenverteilung	Vollständige Daten je Knoten	Knoten mit und ohne vollständige Daten (Selective Nodes)	Vollständige Daten nur bei zentralem Knoten	Smart Contracts und private dezentrale Netze		
Abzuspeichernde Daten	Hashwerte	Code	Dateien			
Informations-freigabe	Keine Begrenzung	Für Adressat der Transaktion und alle Folgenden	Für Adressat der Transaktion	Individuelle Informationsfreigabe		
Lese- und Schreibzugang	Öffentliche Blockchain	Private Blockchain	Konsortium Blockchain			
Regelwerk zur Datenaufnahme	Keine Prüfung der Daten	Nur nach Datenstruktur	Regelwerk nach Knoten	Plausibilitätsprüfung		
Datenablage	Ausschließlich On-chain	Off-chain mit zentraler Datenablage	Off-chain mit verteilter Datenablage			
Bekanntheit der Teilnehmenden	Teilnehmende bekannt	Pseudonymität	Anonymität			
Konsens-algorithmus	Proof of Work (PoW)	Proof of Stake (PoS)	Proof of Authority (PoA)	Practical Byzantine Fault Tolerance Algorithm (PBFT)	Fast Probabilistic Consensus (FPC)	Proof-of-Elapsed-Time (PoET)

5.2 Grad der Datenverteilung

In komplexen Supply-Chains entstehen Daten an sehr vielen Stellen, die wiederum sehr heterogener Art sein können. Eine Datenverteilung ist demnach entsprechend zu wählen, d. h. Menge und Vollständigkeit der Daten sowie die Anzahl der Knoten, die die Daten halten. Sowohl das Schreiben als auch Lesen von Daten sollte den Teilnehmenden der Blockchain und deren Anforderungen angemessen sein. Dabei sind sowohl die Länge von Supply-Chains als auch die Fähigkeiten der Einzelnen zu berücksichtigen; qualitative und rechtliche Ansprüche müssen stets abgedeckt sein.

Vollständige Daten je Knoten

— Hohe Verfügbarkeit von Daten innerhalb der Blockchain.

— Hoher Schutz vor Datenverlust und Manipulation.

— Alle Knoten sind sog. Full-Nodes.

Knoten mit und ohne vollständige Daten (Selective Nodes)

— Light(weight)-Nodes speichern nur den für den Besitzer des Knotens relevanten Teil der Blockchain.

— Light-Nodes sind bei der Verifizierung auf Full-Nodes angewiesen.

— Datenmenge im Blockchain-Netzwerk wird somit reduziert.

Vollständige Daten nur bei zentralem Knoten

— Zentralisierte Datenstruktur.

— Eine Full-Node (z. B. ein zentrales Unternehmen) und sonst nur Light-Nodes, die auf das eine Unternehmen angewiesen sind.

— Sehr geringe Datenmenge im Vergleich zu vollständigen Knoten im gesamten dezentralen Netzwerk.

Smart Contracts und private dezentrale Netze

— Zugangsbeschränkte Subnetze mit bestimmten Validatoren (Konsensbildung zur Akzeptanz von auslösenden Events der Smart Contracts wird nur durch bestimmte Knoten/Teilnehmende im Blockchain-Netzwerk durchgeführt).

— Daten innerhalb der Subnetze sind nicht öffentlich.

— Status und bestimmte Transaktionen können in einem öffentlichen Netz verankert werden.

— Automatisierter Code im Smart Contract ist im Nachhinein nicht änderbar, was großen Validierungsaufwand im Vorfeld bzw. eine mögliche Schwachstelle bedeutet.

Anwenderfreundlichkeit und gemeinsame Datennutzung in Supply-Chains stellen Leitlinien eines Blockchain basierten Datenökosystems dar. Aus der Komplexität der Datenverteilung folgen jedoch Herausforderungen, wie zum Beispiel widersprüchliche Optimierungsziele: Schnelligkeit beim Zugriff steht einer hohen Datenverfügbarkeit entgegen. Genauso ist der Schutz von Daten häufig verzögernd. Aus diesen Gründen wird eine frühe umfassende konzeptionelle Auseinandersetzung über die vielfältigen Optionen empfohlen. Spätere Anpassungen bei der Datenverteilung und -zugriff sind dagegen sehr aufwändig und teuer. Insbesondere gilt dies für die Anlage von Smart Contracts.

5.3 Abzuspeichernde Daten

Welche Daten aus Supply-Chains auf einer Blockchain gespeichert werden sollten, spielt eine zentrale Rolle für Nutzbarkeit und Kosten. Limitierend wirkt dabei besonders die Menge der Daten und somit die Performance. Aber auch eine klare Struktur (Format: vereinbarte Syntax und Semantik) der Daten, die ihre Relevanz für deren Nutzer wiederspiegelt, sind von Bedeutung für die Informationsgewinnung durch die Teilnehmenden der Supply-Chain.

Hashwerte

— Verschlüsselung eines Datensatzes.

— Kann als Pointer (Zeichenfolge, die auf einen Speicherort außerhalb der Blockchain hinweist) verwendet werden. Die Fälschungssicherheit des Hashwerts auf der Blockchain ist trotz einer zentralen Datenhaltung gegeben (Hashwert ändert sich mit Ändern der Daten/ Dokumente). Der Inhalt der Daten/Dokumente kann jedoch nicht überprüft werden, sodass dieser bei einer zentralen Datenhaltung abseits der Blockchain gelöscht und abgestritten werden kann. Es kann lediglich nachgewiesen werden, dass eine Änderung stattgefunden hat.

— Daten selbst sind nicht auf der Blockchain abgelegt.

— (Vergleichsweise sehr geringe Größe).

Code

— Mögliche Implementierung von sog. Smart Contracts.

— Darstellung von Wenn-dann-Beziehungen.

— (Vergleichsweise mittlere Größe, variiert je nach Gestaltung).

Dateien

— Es besteht die Möglichkeit komplette Dateien auf der Blockchain abzuspeichern.

BEISPIEL Textdateien, Audiodateien, oder Bilddateien und Zertifikate.

— (Vergleichsweise sehr groß).

Für eine Verknüpfung von Supply-Chain-Daten aus unterschiedlichen Quellen innerhalb eines Blockchain basierten Datenökosystems ist eine hohe Interoperabilität der abgespeicherten Daten notwendig. Dazu stellen die Vereinbarungen der Blockchain-Teilnehmenden eine Säule der Zusammenarbeit dar. Darüber hinaus können hier offene Standards und OpenSource-Lösungen als Grundlagen dienen.

5.4 Informationsfreigabe

Für die Schaffung von optimaler Transparenz in Supply-Chains gibt es idealerweise keine Begrenzungen für den Informationszugang. Aus technischer Sicht sollten keine Teilnehmenden ausgeschlossen sein. Sehr häufig werden jedoch wirtschaftliche oder rechtliche Gründe für eine Kontrollier- und Steuerbarkeit der Informationsfreigabe verantwortlich gemacht. Grundsätzlich werden Ersteller und Empfänger von Informationen unterschieden. Die Reichweite der Information kann unterschiedlich festgelegt werden.

Keine Begrenzung (zur Erreichung maximaler Transparenz in der Lieferkette)

— Alle Teilnehmenden der Blockchain können die vom Ersteller bereitgestellten Informationen einsehen.

Für Adressat der Transaktion und alle Folgenden

— Der Inhalt der Transaktion ist nur für den Empfänger sowie alle folgenden Teilnehmenden bekannt.

— Soll im Sinne des Schutzes von bspw. Geschäftsgeheimnissen verhindert werden, dass nicht alle nachfolgenden Teilnehmenden alle Informationen erhalten, ist ein Rechtemanagement System notwendig.

Für Adressat der Transaktion

— Charakter des Austauschs von Informationen zwischen zwei Teilnehmenden.

— Mögliche Verschlüsselung durch den Private-Key des Adressaten.

— Reproduktion der Information kann nicht verhindert werden (grundsätzliches Problem und nicht spezifisch für die Blockchain-Technologie).

Individuelle Informationsfreigabe

— Sonderfälle können individuelle Anforderungen darstellen.

BEISPIEL Verschlüsselung jeder Information und anschließende Schlüsselverteilung an betreffende Teilnehmende (siehe 4.2).

— Digitale Identitäten ermöglichen neben einer individuellen Verteilung auch die Verteilung an Gruppen.

Im Sinne der kollaborativen Informationsgewinnung für Partner der Supply-Chain innerhalb einer Blockchain gelten dieselben Umstände und Regeln wie für nicht digital organisierte Netzwerke, die marktwirtschaftlich funktionieren. Mithin ist die Informationsfreigabe stets auch eine Frage von Marktmacht gegen gemeinschaftlichen Wirkens. Die Blockchain-Technologie ist hier lediglich Mittel zum Zweck, sodass die Wirkungsentfaltung

z. B. für Wirtschaft, Umwelt oder Gesellschaft letztlich vom Zusammenhalt aller Teilnehmenden abhängt. Auch eine Unterscheidung von Informationsaustauch unter Partnern, die sich kennen oder anonymen Partnern der Supply-Chain, die sich noch nicht begegnet sind, kann durch Zuhilfenahme von digitalen Identifikatoren (siehe 4.2) ausgeblendet werden.

5.5 Lese- und Schreibzugang

Partner der Supply-Chain können sich auf eine gemeinsame Datennutzung in Blockchains einigen. Dazu sind ihre Lese- und Schreibzugänge zu definieren. Diese unterscheiden sich je nach Ausprägung des Blockchain-Typs: öffentlich, privat oder gemischt. Der gewählte Blockchain-Typ bestimmt in hohem Maße die Organisation des zugehörigen Daten-Ökosystems in seinen wesentlichen Aspekten: Rechtsform, Business-Modell, Governance usw. Der Umgang mit den Daten umfasst die beiden Grundformen: a) Lesezugang: Daten lesen, analysieren oder auditieren und b) Schreibzugang: Berechtigung zur Validierung von neuen Blöcken.

Auch Mischformen der nachfolgend erläuterten Blockchain-Typen sind möglich:

Öffentliche Blockchain

— Lese- und Schreibzugang sind genehmigungsfrei.

Private Blockchain

— Lese- und Schreibzugang sind genehmigungspflichtig.

— Es kann in der Regel auf nicht-triviale Konsensalgorithmen wie beispielsweise Proof-of-Work verzichtet werden, sodass einfachere Verfahren wie Proof-of-Authority oder Practical Byzantine Fault Tolerance Algorithm verwendet werden können (wenn schädliches Handeln durch autorisierte Teilnehmende ausgeschlossen wird). Für eine Erläuterung der Algorithmen siehe 5.9.

— Eine (zentrale) Instanz unterhält die Blockchain.

Konsortium Blockchain

— Hybrider Ansatz zwischen privater und öffentlicher Blockchain.

— Ein Konsortium aus mehreren Teilnehmenden trifft Entscheidung über Verteilung der Lese- und Schreibrechte.

Die genannten beiden Reinformen der Blockchain-Typen stellen Extreme dar, die sich in ihren Funktionalitäten sehr stark unterscheiden. Die Wahl des entsprechenden Blockchain-Typs stellt somit eine der Kardinalentscheidungen für die Gründung eines Daten-Ökosystems für Supply-Chains dar.

5.6 Regelwerk zur Datenaufnahme

Bevor Transaktionen an benachbarte Knoten weitergeleitet werden, sind die Daten nach den im Blockchain-Protokoll festgelegten Kriterien zu überprüfen.

Keine Prüfung der Daten

— Alles wird angenommen.

Nur nach Datenstruktur

— Formatierung der Daten ist zu verifizieren.

— Überprüfen von beispielsweise:

— Syntax und Format der Daten entsprechen den Vorgaben.

— Inputs oder Outputs der Transaktion dürfen nicht null sein.

— Eine Transaktion darf nur eine begrenzte Anzahl von Token übertragen.

Regelwerk nach Knoten

— Überprüft durch Summenbildung die Konsistenz von Wert- oder Zahlenangaben.

BEISPIEL 1 Die neue Transaktion ist erlaubt, wenn die ermittelte Summe der Transaktionsbetrachtung (Inputs und Outputs) größer ist als die Summe der alten.

Plausibilitätsprüfung

— Kontrolle der Daten hinsichtlich ihrer Plausibilität.

BEISPIEL 2 Vorgelagerte Prüfung der Datenstruktur; Eine Eingrenzung der Gesamtmenge von Token, die in einem festgelegten Zeitintervall transferiert werden dürfen; Genauer Regelkatalog muss festgelegt werden.

5.7 Datenablage

Wo werden die Daten gespeichert?

On-chain: Die Daten selbst liegen auf der Blockchain.

Off-chain: Pointer (Hashwert der Daten) wird immer abgelegt, die Daten selbst sind an einem anderen Ort gespeichert.

Ausschließlich On-chain

— Hohe Datenmenge auf der Blockchain (hohe Kosten).

— Zentralisierungsgrad niedrig.

— Durch die Blockchain kryptographisch abgesichert.

Off-chain mit zentraler Datenablage

— Datenmenge auf der Blockchain vergleichsweise gering → bessere Skalierbarkeit.

— Single-Point-of-Failure ist die zentrale Datenablage, die einige Vorteile eines DLT wie hohe Verfügbarkeit und Sicherheit vor Datenverlust aufhebt.

— Zugriffsrechte verteilen.

— Zentralisierungsgrad Hoch (Eine zentrale Partei ist für die Off-Chain Daten zuständig).

Off-chain mit verteilter Datenablage

— Datenmenge auf der Blockchain vergleichsweise gering → bessere Skalierbarkeit.

— Datenablage hat die Hochverfügbarkeit eines verteilten Systems wie die Blockchain.

— Verschlüsselung der Daten bei Ablage kann notwendig sein zur Zugriffskontrolle (Daten liegen auch bei Teilnehmenden, die die Daten nicht einsehen sollen).

5.8 Bekanntheit der Teilnehmenden

Teilnehmende innerhalb des Netzwerkes können sein: Personen, juristische Personen (bspw. Unternehmen), Objekte (bspw. Maschinen, Messstationen). Der Bekanntheitsgrad der Teilnehmenden untereinander kann sein:

Teilnehmende bekannt

— Alle sind bekannt.

Pseudonymität

— „Adresse“ bzw. öffentlicher Schlüssel ist grundsätzlich geschützt, aber da jeder eine feste „Adresse“ im Netzwerk hat, kann ein Profil erstellt werden.

Anonymität

— Komplette Anonymität von Sender und Empfänger.

BEISPIEL Mixing (mehrere Transaktionen aber nur eine ist die „richtige“).

5.9 Konsensalgorithmus

Der Konsensalgorithmus eines DLT stellt sicher, dass alle Knoten im Netzwerk eine einheitliche Verteilung der Tokens auf den Konten als Wahrheit anerkennen. Beispiele für Konsensalgorithmen sind:

Proof of Work (PoW)

— Blockerzeugung ist mit erheblichem Rechen- und Energieaufwand verbunden.

— Rechengeschwindigkeit bestimmt Wahrscheinlichkeit einen neuen Block zu erzeugen.

Proof of Stake (PoS)

— Energieeffiziente Alternative zum PoW.

— Besitz der jeweiligen Währung bestimmt Wahrscheinlichkeit einen neuen Block zu erzeugen.

Proof of Authority (PoA)

— Nur bestimmte Knoten (Validatoren) können entsprechend ihrer Reputation den Konsens bilden.

— Gilt als robuster gegenüber PoS.

— Findet häufige Verwendung in Smart Contracts.

Practical Byzantine Fault Tolerance Algorithm (PBFT)

— Konsistenz sicherstellen, solange mehr als zwei Drittel im Sinne des Netzwerkes arbeiten.

— Nachrichtenaustausch zwischen Knoten stellt Konsistenz sicher.

Fast Probabilistic Consensus (FPC)

— Jeder Knoten hat eine anfängliche Meinung zur Zulässigkeit einer Transaktion, die in mehreren Runden aktualisiert wird, bis eine lokale Stoppregel greift.

— FPC ist auch in Byzantinischen Umgebungen robust.

Proof-of-Elapsed-Time (PoET)

— Intel Software Guard Extension (SGX) generiert für jeden Knoten eine Wartezeit.

— Netzwerkknoten mit der kürzesten Wartezeit gilt als Gewinner und darf den nächsten Block erzeugen.

Für die Wahl der passenden Technologie für ein Vorhaben spielt auch der verwendete Konsensalgorithmus eine Rolle. Die am weitesten verbreiteten Konsensalgorithmen PoW und PoS sind von Natur aus mit Transaktionskosten verbunden. PoW in öffentlichen, genehmigungsfreien Blockchains ist in der Regel mit einem sehr hohen Energieaufwand verbunden. PoS gewichtet den Einfluss auf den Konsens auf die Anzahl an Tokens, die ein Knoten hält. Dies bevorzugt Parteien mit größeren ökonomischen Investitionen, kann aber allen Teilnehmenden ermöglichen, per Staking an den Transaktionsgebühren zu partizipieren.

PoA eignet sich besonders für Fälle, bei denen die Entscheidung einer kleinen Gruppe von vertrauenswürdigen Validatoren überlassen wird. Auch kann es in bestimmten Anwendungsfällen genügen, wenn die Interessenvertreter von Gruppen mit konträren Interessen jeweils einen Validator stellen, um im Konsens das nötige Vertrauen für alle Teilnehmenden zu generieren. Für Lösungen, die in Smart Contracts umgesetzt werden, wird der Konsens innerhalb eines Smart Contracts (also die Entscheidung, wann innerhalb eines Smart Contracts ein Statuswechsel ausgelöst wird) generell durch ein vorbestimmtes “Gremium” erreicht, ein Set an Validator Knoten.

Mit PBFT, FPC und PoET werden DLTs implementiert, die nicht auf die Verwendung von Transaktionsgebühren angewiesen sind. Dies eignet sich besonders, wenn viele Transaktionen und/oder Micropayment relevant ist. FPC hat gegenüber dem PBFT den Vorteil, auch in Byzantinischen Umgebungen robust zu sein.

Ein Vergleich von bestimmten Konsens Algorithmen und Auswahlkriterien für eine Blockchain finden sich z. B. beim Bundesamt für Sicherheit in der Informationstechnik [15].

Anhang A
(normativ)

Lastenheftvorlage für Blockchain- Applikationen in der Supply-Chain

A.1 Blockchain-Applikation für _____

Zum überbetrieblichen Datenaustausch in der Supply-Chain soll eine Blockchain-Applikation zum Einsatz kommen. Als Auftraggeber tritt das folgende Konsortium auf:

Hier sollten alle relevanten Unternehmen mit den jeweiligen Ansprechpartnern gelistet werden. Dabei sollte ein Hauptansprechpartner, der für die Kommunikation mit den Anbietern verantwortlich ist, genannt werden.

1) ***Unternehmensname (Hauptansprechpartner)***

Straße und Hausnummer	
PLZ	
Ort	
Land	

Ansprechpartner

Name, Vorname	
Anschrift	
E-Mail	
Telefonnummer	

2) ***Unternehmensname***

Straße und Hausnummer	
PLZ	
Ort	
Land	

Ansprechpartner

Name, Vorname	
Anschrift	
E-Mail	
Telefonnummer	

A.2 Darstellung und Ausgangssituation

Dieser Abschnitt beschreibt das Ziel des Vorhabens und die Problem-/Aufgabenstellung. Dabei sollte auch darauf eingegangen werden, warum und wofür die Lösung benötigt wird.

Der untenstehende Text ist ein Beispiel und muss auf das Vorhaben angepasst werden.

Um einen fälschungssicheren Austausch von Informationen zwischen sich unbekannten Teilnehmenden in einer Supply-Chain zu ermöglichen, soll eine Blockchain-Applikation aufgesetzt werden. Für die Programmierleistung und Umsetzung der Anforderungen des Auftraggebers sollte eine Dritte Partei beauftragt werden. Die Anforderungen sind in diesem Lastenheft festgehalten.

Aktuell gibt es verschiedene Systeme, Plattformen und Medien zum überbetrieblichen Datenaustausch. In den komplexen Wertschöpfungsstrukturen gibt es außerdem viele unbekannte Partner, die teilweise kein oder nur ein geringes Vertrauen in die bereitgestellten Informationen durch Dritte haben. Informationen zum Sourcing eines Rohstoffes werden bspw. durch eine Vielzahl an Händlern und Unternehmen weitergegeben, sodass der Wahrheitsgehalt im Bezug zu den ursprünglichen Informationen sich oftmals nicht überprüfen lässt. Für einen einheitlichen Datenaustausch und zur Rückverfolgung von Informationen zu Artikeln und Veränderungen soll eine Blockchain zum Einsatz kommen. Dabei ist es vor allem wichtig, eine skalierbare Lösung für sich verändernde Supply-Chains zu gestalten als auch eine individuelle Lösung von Lese- und Schreibrechten zu realisieren, sodass Geschäftsgeheimnisse gewahrt werden können. In der angestrebten Lösung sollen vor allem Informationen zur Nachhaltigkeit von Produkten ausgetauscht werden. Dabei spielen insbesondere Zertifikate zu Materialien, Arbeitsbedingungen, Siegeln usw. eine Rolle.

Das auftraggebende Konsortium deckt dabei die folgenden Stakeholder in der Supply-Chain ab: _____.
Da nicht alle Partner der Supply-Chain von Beginn an mit der Blockchain-Applikation arbeiten werden, wird eine Lösung zum Einpflegen von Daten Dritter (bspw. durch einen ersten Händler, Zertifizierungsunternehmen usw.) benötigt.

A.3 Leistungsbeschreibung/Anforderungen an die Blockchain-Lösung

A.3.1 Grad der Datenverteilung

In komplexen Supply-Chains entstehen Daten an sehr vielen Stellen, die wiederum sehr heterogener Art sein können. Eine Datenverteilung ist demnach entsprechend zu wählen, d. h. Menge und Vollständigkeit der Daten sowie die Anzahl der Knoten, die die Daten halten.

Merkmal	**Trifft zu**
Vollständige Daten je Knoten	
Knoten mit und ohne vollständige Daten (Selective Nodes)	
Vollständige Daten nur bei zentralem Knoten	
Smart Contracts und private dezentrale Netze	

A.3.2 Abzuspeichernde Daten

Abzuspeichernde Daten: Welche Daten auf einer Blockchain gespeichert werden, spielt eine zentrale Rolle. Limitierend wirkt dabei besonders die Größe der Daten und somit die Performance.

Merkmal	Trifft zu
Hashwerte	
Code	
Dateien	

A.3.3 Informationsfreigabe

Die Reichweite der Information kann unterschiedlich festgelegt werden.

Merkmal	Trifft zu
Keine Begrenzung (zur Erreichung maximaler Transparenz in der Lieferkette)	
Für Adressat der Transaktion und alle Folgenden	
Für Adressat der Transaktion	
Individuelle Informationsfreigabe	

A.3.4 Lese- und Schreibzugang

Lesezugang: Daten lesen, analysieren oder auditieren.

Schreibzugang: Berechtigung zur Validierung von neuen Blöcken.

Merkmal	Trifft zu
Öffentliche Blockchain	
Private Blockchain	
Konsortium Blockchain	

A.3.5 Regelwerk zur Datenaufnahme

Bevor Transaktionen an benachbarte Knoten weitergeleitet werden, sind die Daten nach den im Blockchain-Protokoll festgelegten Kriterien zu überprüfen.

Merkmal	Trifft zu
Keine Prüfung der Daten	
Nur nach Datenstruktur	
Regelwerk nach Knoten	
Plausibilitätsprüfung	

A.3.6 Datenablage

Definition des Speicherorts der Daten.

On-chain: Die Daten selbst liegen auf der Blockchain.

Off-chain: Pointer (Hashwert der Daten) wird immer abgelegt, die Daten selbst sind an einem anderen Ort gespeichert.

Merkmal	Trifft zu
Ausschließlich On-Chain	
Off-chain mit zentraler Datenablage	
Off-chain mit verteilter Datenablage	

A.3.7 Bekanntheit der Teilnehmenden

Teilnehmende innerhalb des Netzwerkes können sein: Personen, juristische Personen (bspw. Unternehmen), Objekte (bspw. Maschinen, Messstationen). Der Bekanntheitsgrad der Teilnehmenden untereinander kann sein:

Merkmal	Trifft zu
Teilnehmende bekannt	
Pseudonymität	
Anonymität	

A.3.8 Konsensalgorithmus

Der Konsensalgorithmus eines DLT (Distributed Ledger Systems) stellt sicher, dass alle Knoten im Netzwerk eine einheitliche Verteilung der Tokens auf den Konten als Wahrheit anerkennen.

Merkmal	Trifft zu
Proof of Work (PoW)	
Proof of Stake (PoS)	
Proof of Authority (PoA)	
Practical Byzantine Fault Tolerance Algorithm (PBFT)	
Fast Probabilistic Consensus (FPC)	
Proof-of-Elapsed-Time (PoET)	

A.4 Rand- und Rahmenbedingungen

Dieses Lastenheft bezieht sich auf DIN SPEC 32790 und liegt den Definitionen und Begriffsbestimmungen aus diesem Dokument zugrunde.

1) **Sprachen, in der die Blockchain-Applikation erstellt werden soll**

   1. xxx
   2. xxx
   3. xxx

2) **Cyber-Security-Richtlinien**

   Zur Wahrung der Cyber-Security gelten folgende Regelungen (siehe Anhang):

   1. xxx
   2. xxx
   3. xxx

3) **Weitere Regelungen und Randbedingungen:**

   Hier können Sie alle weiteren, für Sie relevanten Regelungen beschreiben und Anhänge aufführen.

Anhang B
(informativ)

Fallbeispiele

B.1 Fallbeispiel: CO_2-Fußabdruck

Da 80 % des CO_2-Fußabdrucks eines Produktes aus der Lieferkette stammen, können immense Einsparungspotentiale durch einheitliche und verifizierte Weitergabe der Werte aufgedeckt werden. Dies ist heutzutage mit sehr hohem Aufwand verbunden, da nur auf Durchschnittswerte von Datenbanken zurückgegriffen werden kann. Eine einheitliche und verifizierte Berechnung der Werte ist ausschlaggebend für die Dekarbonisierung der Lieferkette und Produkte und wird zu Wettbewerbsvorteilen führen.

Um ein Maximum an Vertrauen für die Primärdaten der Lieferkettenakteure zu gewinnen, können kryptografische Zertifikate über ein Netzwerk ausgetauscht werden. Ein hohes Maß an Datenschutz wird durch die dezentrale Architektur ermöglicht. Bereitgestellte Daten werden verifiziert und die Berechnung des CO_2-Fußabdrucks entlang der gesamten Lieferkette ermöglicht, ohne strategisch relevante Informationen (wie z. B. Produktionsdaten) offenzulegen. Die Daten werden von den Unternehmen ermittelt, durch Dritte verifiziert und können von anderen Teilnehmenden überprüft werden (Verifiable Proof).

Durch die Nutzung von Blockchain ergibt sich die Möglichkeit, verifizierte Werte über verschiedene Branchen hinweg auszutauschen und dadurch einen höheren Grad an Vertrauen zu gewinnen, ohne sensible Daten offenzulegen. Der Aufwand für die Berechnung des CO_2-Fußabdrucks der Lieferkette wird durch automatisierte Verifizierung und Berechnung erheblich reduziert, da Kosten für die manuelle Prüfung von Transaktionen eingespart werden können.

Konkrete Beispiele

CircularTree:

https://www.circulartree.com/projects/carbonblock

Siemens:

https://press.siemens.com/global/de/pressemitteilung/siemens-entwickelt-oekosystembasierten-ansatz-fuer-den-austausch-von

Carbon Future:

https://www.btc-echo.de/schlagzeilen/carbonfuture-start-up-handelt-mit-co2-zertifikaten-ueber-die-blockchain-125247/

Climate CHECK:

https://www.climate-check.com/

B.2 Fallbeispiel: Rückverfolgung von Lebensmitteln

Die Sicherheit der Lebensmittel bezüglich ausreichender Qualität ist heutzutage in Europa eine wichtige Forderung. Gleichzeitig besteht ein vergleichsweise geringes Vertrauen in die Lebensmittelindustrie, dies sicherzustellen. Sind Lebensmittel mit Schadstoffen oder Erregern versetzt, wie beispielsweise bei der EHEC-Epidemie 2012 oder den Fipronil-belasteten Hühnereiern 2017, besteht eine direkte Gefahr beim Verzehr. Die Suche nach Ursachen ist häufig langwierig und aufwendig.

Im Fallbeispiel wurden die Potenziale der Blockchain-Technologie erforscht, um eine IT-Lösung zur lückenlosen Rückverfolgung von Lebensmitteln von der Erzeugung bis hin zum Verkauf zu entwickeln. Die angestrebte Lösung kann ein hohes Maß an Fälschungssicherheit der Daten sicherstellen und bedarf keiner zentralen „dritten" Instanz, beispielsweise eines Plattformanbieters. Dabei wurde untersucht, welche Daten im System erfasst werden müssen und wie es im Sinne der Unternehmen wirtschaftlich auszulegen ist. Die IT-Lösung wird anhand zweier konkreter Anwendungsfälle im Testbetrieb bei Anwendern erprobt.

Die Anforderungen im Bereich der Lebensmittelindustrie, die im Fallbeispiel identifiziert wurden, sind in der entsprechenden Veröffentlichung von Thume 2021 [17] aufgeführt. Insbesondere die Verfügbarkeit und Korrektheit der Daten sowie die Bereitschaft aller Beteiligten die Daten und Informationen zu teilen sind wichtige Anforderungen der Stakeholder in der Supply-Chain.

Eine IT-Lösung sollte Akteure entlang der gesamten Wertschöpfungskette in die Lage versetzen, die für eine lückenlose Rückverfolgung notwendigen Daten zu teilen und im Ereignisfall schneller und effektiver Maßnahmen zum Schutz der Konsumenten einzuleiten. Dies unterstützt die Effektivität von Maßnahmen, wie z. B. gezieltere Rückrufaktionen, wirkt damit einer Verknappung von Lebensmitteln vor und stärkt das Vertrauen der Bevölkerung in die Lebensmittelwirtschaft. Im Bereich der Verarbeitung von Supply-Chain-Events in der Lebensmittelrückverfolgung kann EPCIS 2.0 [18], als Neuauflage des etablierten EPCIS, angewendet werden.

Konkrete Beispiele

Sichere Lebensmittelkette durch Anwendung der Blockchain-Technologie (SILKE):

https://www.projekt-silke.de/

EPCIS Standard 2.0, *(2022, Version 2.0):*

https://ref.gs1.org/standards/epcis/

B.3 Fallbeispiel: Lieferkette Luft- und Raumfahrt und Automobilindustrie

Sowohl Luft- und Raumfahrt- als auch Automobilindustrie schreiben über DIN EN 9100 [19] bzw. IATF 16949 [20] eine lückenlose Rückverfolgbarkeit von Daten und Produkten innerhalb der Lieferkette verpflichtend vor. Die Archivierungsvorgaben hinsichtlich Datensicherheit, Manipulationssicherheit und Archivierungsfristen (typisch sind min. 15 Jahre bis 50 Jahre, je nach Anwendung und Kundengruppe) verlangen im digitalen Zeitalter nach neuen Lösungen. In zunehmendem Maß müssen sich beide Industrien nachweislich auch in Richtung von mehr Nachhaltigkeit in den Produktionsprozessen und eingesetzten Werkstoffen entwickeln.

Bei der Konstruktion eines Fahr-/Flugzeugs werden viele verschiedene Teile verbaut, die von unterschiedlichen Herstellern und Zulieferern stammen. Diese Bauteile unterliegen strengen Qualitäts- und Qualifizierungsanforderungen, da sie maßgeblich zu der Sicherheit des Endproduktes beitragen. Ausgiebige unabhängige Tests sind notwendig, um die Erfüllung der Qualitätsstandards nachzuweisen. Auch gilt es gesetzliche Regelungen hinsichtlich der Beschaffung und deren Rückverfolgbarkeit sowie Dokumentation von Vormaterial-Lieferketten (Beispiel „Konfliktrohstoffe") zu erfüllen. Und nicht zuletzt müssen Themen wie Dokumentation und Transparenz von CO_2-Emissionen, Kreislaufwirtschaft und Recyclingquoten adressiert werden.

Mittels Blockchain-Lösung sind Lieferwege, Zertifikate, Siegel und Prüfungen und damit umfassende Qualitätsdaten systematisch nachvollziehbar und transparent einsehbar. Eine nachträgliche Veränderung/Manipulation von Datensätzen ist nicht möglich. Erste Pilotprojekte zu diversen Teilthemen wurden bereits durchgeführt.

Es gibt ausgesprochen vielversprechende Ansätze auf nationaler und internationaler Ebene zur Lösung der sehr komplexen Anforderungen. Dabei wird sich auf die Vernetzung von Lieferketten sowie Digitalisierung und Zertifizierung von Produkten und Prozessen konzentriert.

Über durchgängige Datenketten für relevante Wertschöpfungsprozesse sollen Daten-Ökosysteme möglich werden, die vielfältige Vorteile für die Netzwerkpartner schaffen. Das setzt technische Möglichkeiten sowie Kooperationswillen der Partner voraus. Wesentliche Stichworte hierzu sind technischer Konsens der Akteure, Tech-

nologieoffenheit, Interoperabilität der Systeme sowie die Schaffung von Industriestandards. Schlussendlich wird dadurch eine Integration der Lieferkette (OEM/Klein- und Mittelstand) und der damit erzielbaren Vorteile, wie z. B. einer Verbesserung der Resilienz, der Innovationskraft aber auch der Ertragschancen, ermöglicht.

Bestes Beispiel aus der Luft- und Raumfahrt ist die DIN SPEC 9012 [21], die das digitale Datenaustauschformat für Qualitätsdokumente definiert (https://e-coc.org/).

Dazu zählen Konformitätszeugnisse, Prüfbescheinigungen, Bemusterungsunterlagen, ergänzende Lieferdokumente usw. Mittels des e-CoC können benötigte Daten zielsicher, schnell und mit minimalem Aufwand identifiziert und verarbeitet werden, da sie maschinenlesbar sind. Und diese Qualitätsdaten werden zunehmend ergänzt durch Nachhaltigkeitsdaten.

BEISPIEL CO_2-Fußabdruck des Rohstoffs Aluminium, die Recyclingquote, Angaben zu emissionsreduzierten Prozessen, die Rohstoffherkunft selbst u. v. m. sollen erfasst und innerhalb der Supply-Chain manipulationssicher kommuniziert und dokumentiert werden.

Eine bekannte Initiative aus dem Automobilbau ist Catena-X, die sich als ein schnell skalierbares erweiterbares Ökosystem, an dem sich alle Teilnehmende der automobilen Wertschöpfungskette beteiligen können, versteht. Das Ziel ist, eine Umgebung für den Aufbau, den Betrieb und die kollaborative Nutzung durchgängiger Datenketten entlang der gesamten automobilen Wertschöpfungskette zu schaffen. Die Integration mit GAIA-X über eine im GAIA-X-Knoten verknüpfte Blockchain-Technologie führt zu zusätzlicher Sicherheit und Unabhängigkeit bei der Verwaltung von Daten (https://catena-x.net/de/).

Die Stakeholder in beiden genannten Beispielen (DIN SPEC 9012 und Catena-X) sind entlang der gesamten Wertschöpfungskette zu finden. Dies können Produktionspartner, Kunden, Entwicklungspartner, Softwarepartner, Finanzpartner, Logistikpartner, Mobilitätspartner, Recyclingpartner usw. sowie die jeweiligen Funktionen und Abteilungen in den jeweiligen Unternehmen wie z. B. Einkauf, Qualität, Produktion, Vertrieb usw. sein.

Konkrete Beispiele

Digitale Konformitätsbescheinigung (e-CoC):

https://e-coc.org/

Catena-X Automotive Network:

https://catena-x.net/de/

B.4 Fallbeispiel: Konfliktrohstoffe

Seit 08. Juni 2017 ist die sogenannte Conflict Minerals Regulation der Europäischen Union (Verordnung (EU) 2017/821) für die Sorgfaltspflicht bestimmter Ressourcen in der Lieferkette [22] in Kraft. Die Einstufung dieser Rohstoffe als kritisch oder konfliktbehaftet entsteht durch die Knappheit auf den Weltmärkten sowie durch das Risiko regionaler Konflikte, z. B. unzumutbare Arbeitsbedingungen im Bergbau. Seit 1993 hat sich die Anzahl der im Kleinbergbau beschäftigten Arbeiter verdreifacht, wobei ein Großteil informell beschäftigt sind und ausbeuterischen Arbeitsbedingungen ausgesetzt sind.

Daher ergibt sich eine große Verantwortung für Unternehmen entlang der Wertschöpfungskette, dafür Sorge zu tragen, dass ihre Lieferketten von solchen Konflikten befreit sind.

Durch die Erstellung eines digitalen Zwillings der Rohmaterialien können diese digital entlang der Lieferkette rückverfolgt werden. Teilnehmende eines Blockchain Netzwerks können Due-Diligence Daten über die Herkunft der Rohstoffe austauschen, ohne sensible Unternehmensdaten teilen zu müssen. EU-Importeure können eine solche Anwendung nutzen, um internationale Vorschriften zu erfüllen und dadurch Risiken zu minimieren und die Lieferung von Rohstoffen sicherzustellen.

Die Schaffung eines auf der Blockchain-Technologie basierenden Ökosystems ermöglicht es Unternehmen, zu überprüfen, ob alle Akteure OECD-konform handeln. Dies wird den Weg für neue Anreizmodelle ebnen, die die Nachfrage nach Mineralien und Metallen anregen, die verantwortungsvoll bezogen werden.

Konkrete Beispiele

CircularTree:

https://www.sustainblock.org

IOTA:

https://blog.iota.org/trusted-supply-chain-for-conflict-free-resources/

B.5 Fallbeispiel: Papierlose Zollabfertigung

Der internationale Handel ist im Wesentlichen ein informationsintensiver Vorgang, der die Erzeugung, Übermittlung und Speicherung dieser Informationen als kritischen Erfolgsfaktor für den Handel erfordert. Eine der größten Herausforderungen, die die internationalen Handelsströme beeinträchtigen, ist der grenzüberschreitende Informationsaustausch zwischen den Handelsakteuren. Das Fehlen eines integrierten Rahmens für den grenzüberschreitenden Informationsaustausch macht die Sichtbarkeit von Waren und Dienstleistungen im Transit praktisch unmöglich, so dass kein einzelner Akteur in der Handelslieferkette in der Lage ist, genau zu erfassen, was gehandelt wird. Die Informationen, die zur Unterstützung der Handelslieferkette über die Grenzen hinweg ausgetauscht werden, erfolgen hauptsächlich über Dritte, wobei manuelle Dokumente verwendet werden, die fälschungsanfällig sind und häufig nicht mit der Bewegung der jeweiligen Waren und Dienstleistungen synchronisiert sind. Der bestehende Rahmen für den grenzüberschreitenden Austausch von Handelsinformationen ist kostspielig, ineffizient und ungenau, und es mangelt an Transparenz. Die Art und Weise, wie die Dokumente erstellt und an/von den Bestimmungs-/Quellmärkten übermittelt werden, hat Zweifel aufkommen lassen, da es Fälle von Betrug und/oder Verlust von Dokumenten gegeben hat. Die daraus resultierenden Verzögerungen im Prozess haben Auswirkungen auf die Haltbarkeit und damit auf die Wettbewerbsfähigkeit dieser Güter.

Ziel ist eine integrierte Lösung für den Austausch von Informationen an der Quelle, so dass keine Notwendigkeit besteht, sich auf Dritte zu verlassen. Die Primärinformationen zu jeder Transaktion werden an der Quelle generiert und übermittelt, und alle anderen Teilnehmenden nutzen diese Primärinformationen, um einen Mehrwert zu schaffen oder ihre Aufträge innerhalb und über die Grenzen hinweg auszuführen. Zwei weitere Erfolgsfaktoren sind der freie Zugang zur Lösung und die Anerkennung in den Transitländern. Beispielsweise haben in ganz Ostafrika die Zollverwaltungen von fünf Ländern im Rahmen des einheitlichen Zollgebiets bereits eine Regelung für den Informationsaustausch eingeführt, die auf einem regional vereinbarten, durch ICT unterstützten Betriebsrahmen beruht und die angestrebte Lösung zulässt. Entsprechende Vereinbarungen gilt es mit den Zielländern zu treffen.

Mit einem DLT basierten System, bei dem es nicht mehr notwendig ist, physische Dokumente innerhalb und über die Grenzen hinweg auszutauschen, sich auf Drittquellen zu verlassen und langwierige Überprüfungsverfahren durch die Behörden durchzuführen, lassen sich die beschriebenen Probleme lösen. Studien haben gezeigt, dass einer der Gründe, warum ostafrikanische Waren länger in europäischen Häfen auf die Abfertigung warten, mit der Dokumentation zusammenhängt — zum Beispiel wird brasilianischer Kaffee nach Europa schneller abgefertigt als ugandischer Kaffee, und die Hauptursache für diesen Unterschied ist der Dokumentationsprozess, den ugandischer Kaffee im Vergleich zu anderen Kaffeesorten durchlaufen muss. Solche Diskrepanzen werden durch solch ein System beseitigt, das den europäischen Behörden und Unternehmen Echtzeit- und zuverlässige Informationen über den Inhalt und die Art der Kaffeeexporte aus Uganda zur Verfügung stellen wird. Weitere angestrebte Resultate:

— Bessere Sichtbarkeit von Waren im Transit. Mehr Akteure werden jederzeit Zugang zu Echtzeit- und rückverfolgbaren Informationen in einer Handelslieferkette haben.

— Verfügbarkeit zuverlässiger Vorabinformationen für die Akteure der Rückverfolgung. Für den Zoll wäre dies von unschätzbarem Wert, insbesondere für die Steuerverwaltung.

— Verstärkte Zusammenarbeit zwischen den Regierungen und zwischen den Unternehmen. Dies wird möglich, da der Informationsaustausch auf Informationen beruht, die aus der primären Quelle stammen und denen man vertrauen kann. Bietet z. B. die Möglichkeit, Mehrwertdienste anzubieten.

— Verringerung des Zeit- und Kostenaufwands für die Beförderung von Waren vom Ursprungsland zu den Zielmärkten und umgekehrt.

— Verbesserung der Wettbewerbsfähigkeit der Herstellerregion bei Waren, die die Region in verschiedene Zielländer exportiert.

Konkrete Beispiele

IOTA:

https://blog.iota.org/trademark-east-africa-and-iota-paperless-trade-with-the-tangle-aims-to-become-a-standard-in-2022/

Project Brief TMEA:

https://www.trademarkea.com/project/trade-logistics-information-pipeline-tlip/

B.6 Fallbeispiel: Zertifiziertes Kunststoffrezyklat

Angesichts des sich beschleunigenden Wandels im umweltfreundlichen Verbraucherverhalten stehen Marken zunehmend unter Druck, geeignete Maßnahmen zu ergreifen und recycelte Kunststoffe einzusetzen – doch ihre Bemühungen stoßen auf erhebliche Hindernisse. Zwar werden jedes Jahr Millionen von Tonnen Plastik entsorgt, doch auf dem Weltmarkt herrscht ein erheblicher Mangel an hochwertigem recyceltem Kunststoff.

Organisationen suchen nach Wegen, ihre Umweltbilanz zu verbessern und ihre Selbstverpflichtungen zu erfüllen. Empower Plastic Credits ermöglicht es Aktivitäten zur Plastikbeseitigung auf der ganzen Welt zu finanzieren. Dies hilft nicht nur bei der Beseitigung der Umweltverschmutzung durch Plastik, sondern schafft auch ein Einkommen für benachteiligte Gruppen.

Durch die Blockchain-gestützte Rückverfolgung kann der gesammelte Kunststoff vollständig zertifiziert, standardisiert und auf dem globalen Markt verkauft werden. Die Rückverfolgung umfasst auch einen fotografischen Beweis für jede Säuberungsaktion – so haben Käufer von Plastic Credits eine handfeste Möglichkeit, ihren Beitrag zum Umweltschutz zu belegen und der Welt mitzuteilen.

Die Blockchain ermöglicht die lückenlose Verfolgung und Monetarisierung von Kunststoff, sogar in Ländern der Dritten Welt, in denen die überwiegende Mehrheit der Bevölkerung keine Bankverbindung hat. Durch die Verfolgung jedes Teilaspekts des Materialstroms – von der Kunststoffsammlung vor Ort bis hin zur Wiederverwendung in neuen Produkten – wird ein Maß an Transparenz erreicht, das für Marken, Kunststoffverarbeiter und Endverbraucher attraktiv ist.

Konkrete Beispiele

Empower.Eco:

https://www.empower.eco/de/

Literaturhinweise

[1] Rodenhäuser, B.; Rauch, C., (2015): Supply Chain 2025. Eine Studie des Zukunftsinstituts für den Verband der Wellpappen-Industrie. Hrsg.: Zunkunftsinstitut GmbH. S. 7 – 9. [online] URL: https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/VDW_Zukunftsstudie-Supply-Chain-2025.pdf

[2] Hermes Germany GmbH, (2020): Nachhaltigkeit im Supply Chain Management. S. 2. [online] URL: https://www.hermes-supply-chain-blog.com/wp-content/uploads/2020/04/Hermes-Barometer-12-Nachhaltigkei-im-SCM.pdf

[3] Schuh, G.; Prote, J.-P.; Dany, S., (2017): Internet of Production. In: Internet of Production für agile Unternehmen. AWK Aachener Werkzeugmaschinen-Kolloquium 2017, 18. bis 19. Mai. Hrsg.: C. Brecher; F. Klocke; R. Schmitt; G. Schuh. 1. Auflage. Apprimus Verlag, Aachen 2017, S. 1 – 11.

[4] Bauernhansl, T.; Hompel, M.; Vogel-Heuser, B. (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration. Springer Vieweg, Wiesbaden 2014. S. 574.

[5] Lu, T.; Guo, X.; Xu, B.; Zhao, L.; Peng, Y.; Yang, H. (2013): Next Big Thing in Big Data: The Security of the ICT Supply Chain. In: 2013 International Conference on Social Computing. Hrsg.: International Conference on Social Computing. IEEE 08.09.2013 — 14.09.2013, S. 1066 – 1073.

[6] Schuh, G.; Anderl, R.; Gausemeier, J.; Hompel, M.; Wahlster W. (2017): Industrie 4.0 Maturity Index. Die digitale Transformation von Unternehmen gestalten (acatech STUDIE). Hrsg.: G. Schuh; R. Anderl; J. Gausemeier; M. ten Hompel; Wahlster W.Herbert Utz Verlag, München 2017. S. 28 - 29

[7] Schlatt, V.; Schweizer, A.; Urbach, N.; Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Hg. v. Fraunhofer FIT. S. 8.

[8] Badev, A. I.; Chen, M. (2014): Bitcoin: Technical Background and Data Analysis. FEDS Working Paper No. 2014-104. In: SSRN Journal (104), pp. 1–38. S. 9. DOI: 10.2139/ssrn.2544331

[9] Siegel, D. (2017): Blockchain — Begriff, Potenziale, Bewertung. In: WIST 46 (12), S. 45 – 47. DOI: 10.15358/0340-1650-2017-12-45

[10] ISO 22739:2020, *Blockchain and distributed ledger technologies — Vocabulary*

[11] Holtkemper, D. (2020): Blockchain-Applikation für das Supply-Chain-Management. S. 94 f.

[12] W3C Recommendation (2022): Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. [online] URL: https://www.w3.org/TR/did-core/; zuletzt geöffnet am 28.04.2022; Eigenübersetzung

[13] Caldarelli, G.: Understanding the Blockchain Oracle Problem: A Call for Action. Information 2020, 11, 509. https://doi.org/10.3390/info11110509

[14] The Linux Foundation, (2021): Projekt Alvarium. [online] URL: https://wiki.lfedge.org/display/LE/Project+Alvarium

[15] Bundesamt für Sicherheit in der Informationstechnik, (2019): Blockchain sicher gestalten – Konzepte Anforderungen, Bewertungen. [online] URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf

[16] DSGVO, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung —

DSGVO). [online] URL:
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[17] Thume M.; Lange J.; Unkel M. P.; Prange A.; Schürmeyer M., (2021): Blockchain-based traceability in the food industry: requirements analysis along the food supply chain, [online] URL: https://osf.io/uyb64/

[18] EPCIS Standard 2.0, *(2022, Version 2.0). Hrsg: GS1. [online]* URL: https://ref.gs1.org/standards/epcis/

[19] DIN EN 9100, *Qualitätsmanagementsysteme — Anforderungen an Organisationen der Luftfahrt, Raumfahrt und Verteidigung*

[20] IATF 16949, *Anforderungen an Qualitätsmanagementsysteme für die Serien- und Ersatzteilproduktion in der Automobilindustrie*

[21] DIN SPEC 9012, *Luft- und Raumfahrt — Digitale Konformitätsbescheinigung (e-CoC) — Anforderungen, Gestaltung und Aufbau; Text Englisch*

[22] Verordnung (EU) 2017/821 des Europäischen Parlaments und des Rates vom 17. Mai 2017 zur Festlegung von Pflichten zur Erfüllung der Sorgfaltspflichten in der Lieferkette für Unionseinführer von Zinn, Tantal, Wolfram, deren Erzen und Gold aus Konflikt- und Hochrisikogebieten. [online] URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32017R0821&from=EN

Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (LkSG). [online] URL: https://www.gesetze-im-internet.de/lksg/

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), (2019): White Paper — Blockchain in Trade Facilitation, Version 2. [online] URL:
http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI), Fraunhofer-Institut für angewandte Informationstechnik (FIT), (2019): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. [online] URL:
https://www.fit.fraunhofer.de/de/geschaeftsfelder/kooperationssysteme/blockchain/blockchain-grundgutachten-bmvi.html

Jonasson, P., Board, E.; Clemens, R.; van der Wilden, E.; Voorspuij, J. (2020): Sustainable post-COVID-19 supply chain recovery through global data standards — Building a resilient supply chain through product identification and data sharing. [online] URL:
https://www.unescap.org/sites/default/files/113%20Final-Team%20Patrik%20Jonasson-GS1.pdf

Fallbeispiel CO2-Fußabdruck

CircularTree: Carbonblock. [online] URL: https://www.circulartree.com/projects/carbonblock

Project Carbonblock: Value Chain Carbon Transparency Pathfinder Enabling decarbonization through Scope 3 emissions transparency (2021). Hrsg: World Business Council for Sustainable Development [wbcsd). [online] URL: https://www.wbcsd.org/Programs/Climate-and-Energy/Climate/SOS-1.5/Resources/Value-Chain-Carbon-Transparency-Pathfinder-Enabling-decarbonization-through-Scope-3-emissions-transparency

Siemens AG: Ökosystembasierter Ansatz für den Austausch von Emissionsdaten (Pressemitteilung). [online] URL: https://press.siemens.com/global/de/pressemitteilung/siemens-entwickelt-oekosystembasierten-ansatz-fuer-den-austausch-von

Stede C. (2021): Carbonfuture: Start-up handelt mit CO2-Zertifikaten über die Blockchain. In: BTC-Echo [online] URL: https://www.btc-echo.de/schlagzeilen/carbonfuture-start-up-handelt-mit-co2-zertifikaten-ueber-die-blockchain-125247/

Climate CHECK. [online] URL: https://www.climate-check.com/

Fallbeispiel: Rückverfolgung von Lebensmitteln

Sichere Lebensmittelkette durch Anwendung der Blockchain-Technologie (SILKE). [online] URL: https://www.projekt-silke.de/

EPCIS Standard 2.0, *(2022, Version 2.0). Hrsg: GS1. [online]* URL: https://ref.gs1.org/standards/epcis/

Fallbeispiel: Lieferkette Luft- und Raumfahrt und Automobilindustrie

DIN SPEC 9012 Digital Certificate of Conformity (e-CoC). [online] URL: https://e-coc.org/

Catena-X Automotive Network. [online] URL: https://catena-x.net/de/

Fallbeispiel: Konfliktrohstoffe

CircularTree: SustainBlock. [online] URL: https://www.circulartree.com/projects/sustainblock

Project SustainBlock: Blockchain-assisted Mineral Supply Chain Due Diligence. Hrsg: iPoint-systems [online] URL: https://www.sustainblock.org

Schütze. E.: Trusted Supply Chain for Conflict: Tracing Raw Materials with IotaOrigin. Hrsg: IOTA Foundation. In IOTA Blog. [online] URL: https://blog.iota.org/trusted-supply-chain-for-conflict-free-resources/

Fallbeispiel: Papierlose Zollabfertigung

Lund-Nielsen, J. M.: Trademark East Africa and IOTA: Paperless Trade with the Tangle Aims to Become a Standard 2022. Hrsg: IOTA Foundation. In: IOTA Blog. [online] URL: https://blog.iota.org/trademark-east-africa-and-iota-paperless-trade-with-the-tangle-aims-to-become-a-standard-in-2022/

Project Brief: Trade Logistics Information Pipeline (TLIP). Hrsg: TradeMark East Africa (TMEA). [online] URL: https://www.trademarkea.com/project/trade-logistics-information-pipeline-tlip/

Fallbeispiel: Zertifiziertes Kunststoffrezyklat

empower.eco: Recycling von Kunststoffabfällen. Hrsg.: EMPOWER AS [online] URL: https://www.empower.eco/de/