

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.

Inhalt

	Seite
Vorwort	4
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Inhaltliche Einführung	7
4.1 Blockchain	7
4.2 Dezentrale digitale Identifikatoren – Decentralized Identifiers (DIDs)	8
4.3 Anforderungen an Blockchain-Applikationen in Supply-Chains	8
4.4 Anwendungsfälle	9
4.5 Technische Grenzen — das Orakelproblem	10
5 Referenzarchitektur — Taxonomie einer Blockchain-Applikation	10
5.1 Allgemeines	10
5.2 Grad der Datenverteilung	11
5.3 Abzuspeichernde Daten	12
5.4 Informationsfreigabe	13
5.5 Lese- und Schreibzugang	14
5.6 Regelwerk zur Datenaufnahme	14
5.7 Datenablage	15
5.8 Bekanntheit der Teilnehmenden	16
5.9 Konsensalgorithmus	16
Anhang A (normativ) Lastenheftvorlage für Blockchain- Applikationen in der Supply-Chain	18
A.1 Blockchain-Applikation für _____	18
A.2 Darstellung und Ausgangssituation	19
A.3 Leistungsbeschreibung/Anforderungen an die Blockchain-Lösung	19
A.3.1 Grad der Datenverteilung	19
A.3.2 Abzuspeichernde Daten	20
A.3.3 Informationsfreigabe	20
A.3.4 Lese- und Schreibzugang	20
A.3.5 Regelwerk zur Datenaufnahme	20
A.3.6 Datenablage	20
A.3.7 Bekanntheit der Teilnehmenden	21
A.3.8 Konsensalgorithmus	21
A.4 Rand- und Rahmenbedingungen	22
Anhang B (informativ) Fallbeispiele	23
B.1 Fallbeispiel: CO ₂ -Fußabdruck	23
B.2 Fallbeispiel: Rückverfolgung von Lebensmitteln	23
B.3 Fallbeispiel: Lieferkette Luft- und Raumfahrt und Automobilindustrie	24
B.4 Fallbeispiel: Konfliktrohstoffe	25
B.5 Fallbeispiel: Papierlose Zollabfertigung	26
B.6 Fallbeispiel: Zertifiziertes Kunststoffrezyklat	27
Literaturhinweise	28

Bilder

Bild 1 — Integration von Blockchain-Technologie in bestehende IT-Systeme	9
--	---

Tabellen

Tabelle 1 — Taxonomie einer Blockchain-Applikation 11

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, CO₂-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 22739¹, *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 Schlüssel 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 Sovereign 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.

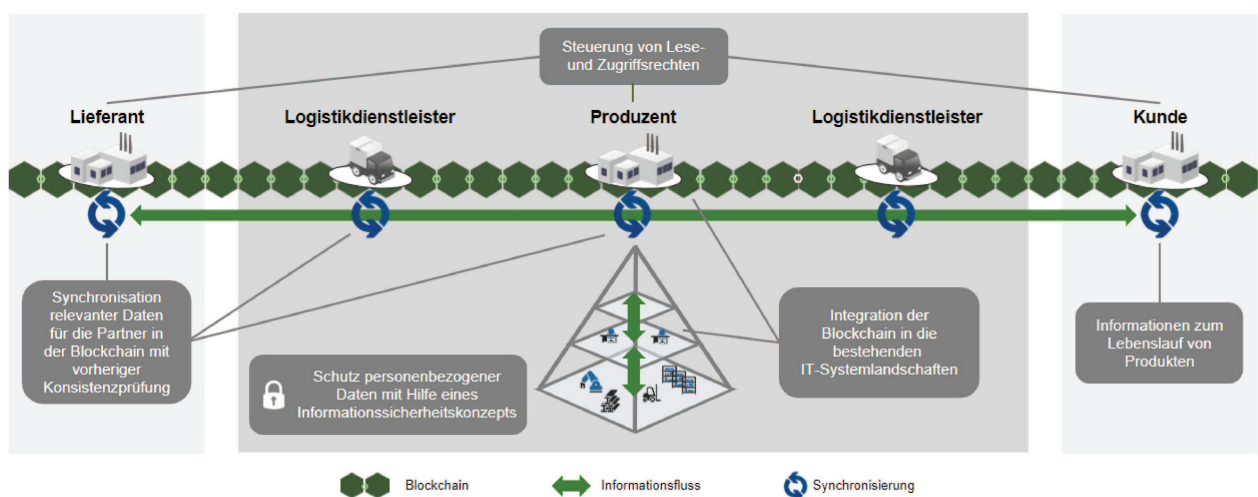


Bild 1 — Integration von Blockchain-Technologie in bestehende IT-Systeme

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 CO₂-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: