

Schlussbericht vom 15.03.2023

zu IGF-Vorhaben Nr. 21256N

Thema

ABCChain – Anwendungsorientierte Blockchain-Applikationen im Supply-Chain-Management

Berichtszeitraum

01.07.2020 - 30.09.2022

Forschungsvereinigung

FIR e. V. an der RWTH Aachen

Forschungseinrichtung

FIR e. V. an der RWTH Aachen

Autoren

Tobias Schröer, FIR e. V. an der RWTH Aachen

Jokim Janßen, FIR e. V. an der RWTH Aachen

Jessica Rahn, FIR e. V. an der RWTH Aachen

Gefördert durch:

Inhalt

Abbildungsverzeichnis.....	3
Tabellenverzeichnis.....	4
1 Einleitung	5
1.1 Zielstellung des Projekts	6
1.2 Projektplan und -verlauf	7
2 Durchgeführte Arbeiten und Ergebnisse.....	10
2.1 AP 1: Anforderungen an Blockchain-Applikationen	10
2.2 AP 2: Blockchain-Referenzarchitektur	14
2.3 AP 3: Identifikation von Daten und Schnittstellen	25
2.4 AP 4: Standardisierung in einer DIN SPEC	27
2.5 AP 5: Gestaltungsleitfaden zur Integration einer Blockchain-Applikation	33
2.6 AP 6: Validierung der Ergebnisse.....	37
3 Wissenschaftlich-technischer und wirtschaftlicher Nutzen für KMU.....	43
4 Fortschreibung des Ergebnistransfers und Einschätzung der Realisierbarkeit des Transferkonzepts.....	44
Literaturverzeichnis.....	47

Abbildungsverzeichnis

Abbildung 1: Überblick über die Arbeitspakete des Forschungsprojekts ‚ABChain‘	9
Abbildung 2: Anforderungen an Blockchain-Applikationen.....	13
Abbildung 3: Anwendungsfälle für den Einsatz einer Blockchain-Applikation im SCM	14
Abbildung 4: Morphologie der Blockchain-Technologie	16
Abbildung 5: Grad der Datenverteilung.....	17
Abbildung 6: Abzuspeichernde Daten.....	19
Abbildung 7: Informationsfreigabe	20
Abbildung 8: Informationsfreigabe	21
Abbildung 9: Relevante Daten, die über eine Blockchain-Applikation geteilt werden	26
Abbildung 11: Auszug aus der DIN SPEC 32790	30
Abbildung 12: Angepasste Morphologie der Blockchain-Technologie für die DIN SPEC 32790	30
Abbildung 13: Vorgehen zur Auswertung	35
Abbildung 14: Angepasste Morphologie für die Fallstudie Projekt Silke.....	40
Abbildung 15: Angepasste Morphologie für die Fallstudie Projekt Anonymes Herstellungsunternehmen	41

Tabellenverzeichnis

Tabelle 1: Interviewleitfaden.....	12
Tabelle 2: Auszug über existierende Normen, Standards und laufende Aktivitäten	28
Tabelle 3: Entwicklungsprozess der DIN SPEC.....	29
Tabelle 4: Fragebogen des Gestaltungsleitfaden.....	34
Tabelle 5: Merkmale bzgl. Auswertung.....	36
Tabelle 6: Darstellung des durchgeführten Validierungsgespräch	39
Tabelle 7: Wissenschaftlich-technischer Personaleinsatz des Forschungsinstituts FIR	43
Tabelle 8: Leistungen Dritter.....	43
Tabelle 9: Ergebnistransfer während der Projektlaufzeit.....	47
Tabelle 10: Ergebnistransfer nach dem Projektzeitraum.....	48

1 Einleitung

Nachhaltiges Wirtschaften und verantwortungsvoller Umgang mit Ressourcen und Umwelt haben in der deutschen Gesellschaft und so auch für Unternehmen einen hohen Stellenwert erlangt (s. RODENHÄUSER; RAUCH 2015, S. 7; HERMES GERMANY GMBH 2020). Um Aussagen über die Produkte treffen zu können, müssen die Unternehmen die entsprechenden Informationen über die gesamte Lieferkette aufnehmen und weitergeben, was nur mithilfe von Transparenz umgesetzt werden kann (s. RODENHÄUSER 2015, S.5; RAUCH 2015, S. 9). So kann Kunden die geforderte Einsicht in die Lieferkette gewährleistet werden und sie können z. B. über Nachhaltigkeitszertifikate über Produktionsbedingungen und die Herkunft der Produkte informiert werden. Mit der stärkeren Verflechtung der Unternehmen und dem Austausch umfassender, teilweise sensibler Daten gewinnen auch die Themen Datensicherheit und Datenschutz an Relevanz (s. LU ET AL. 2013, S. 1067). 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 (s. SCHUH ET AL. 2017, S. 28f.).

Die technologische Grundlage für das Ziel der Transparenz und die genannten Herausforderungen bietet die Blockchain. Als verteilte Datenbank mit außerordentlicher Datensicherheit, Verfügbarkeit von Informationen in Echtzeit im gesamten Netzwerk und hoher Verlässlichkeit kann sie die Kriterien erfüllen (s. SIEGEL 2017, S. 45). Daten zu Emissionen, Arbeitsbedingungen, Materialherkunft und weiteren Nachhaltigkeitskriterien können so entlang der Lieferkette aufgenommen und verteilt werden. Im Forschungsprojekt ‚ABChain‘ wird deshalb untersucht, wie eine Blockchain-Applikation im Supply-Chain-Management aufgebaut sein muss, um den Anforderungen durch die beteiligten Stakeholder sowie den technologischen Rahmenbedingungen der Blockchain zu entsprechen.

Um die Eignung der Blockchain nachvollziehen zu können, sollen im Folgenden die technologischen Grundlagen der Blockchain erläutert werden:

Nach SCHLATT ET AL. 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. Die Nutzung der Hash-Funktionen in einer Blockchain schließt es somit praktisch aus, dass Daten manipuliert oder gelöscht werden. (s. SCHLATT ET AL. 2016, S. 8; s. BADEV ET AL. 2014, S. 9) Die Echtheit der Information wird zudem durch ein mathematisches Schlüsselpaar sichergestellt. Der Versender der Information signiert mit seinem persönlichen Schlüssel; daraufhin kann der Empfänger die Daten mit dem zum Versender passenden Schlüssel öffnen (s. SCHLATT ET AL. 2016, S. 8). So kann die Manipulation von Informationen im Nachhinein nicht

unentdeckt erfolgen und die Authentizität der Informationen kann garantiert werden. Die Sicherheit gegen den Datenverlust wird durch die dezentrale Speicherung bei einer ausreichenden Anzahl an Netzknoten gewährleistet (s. SIEGEL 2017, S. 45). 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 für einen permanenten Verlust 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.

Die rein technologische Eignung der Blockchain für den Einsatz im Supply-Chain-Management (SCM) reicht jedoch nicht aus, um die Potenziale effizient zu nutzen. Aus diesem Grund soll eine anwendungsfallsspezifische Blockchain-Architektur entwickelt werden, die die Anforderungen der Anwendenden und Anbietenden berücksichtigt.

1.1 Zielstellung des Projekts

Das Forschungsvorhaben ‚ABChain‘ zielt darauf ab, kleine und mittlere Unternehmen (KMU) in zunehmend komplexeren Wertschöpfungsnetzwerken mit steigenden Ansprüchen an Datensicherheit und immer kürzeren Produktlebenszyklen zur Nutzung und Integration von Blockchainapplikationen (BC-Applikationen) im Supply-Chain-Management zu befähigen. Die Blockchain als verteilte Datenbank mit außerordentlicher Datensicherheit, Verfügbarkeit von Informationen in Echtzeit im gesamten Netzwerk und hoher Verlässlichkeit bietet dabei die technologische Grundlage, um insbesondere Zuliefer- und Logistikunternehmen bei bereits bestehenden und sich entwickelnden Herausforderungen der Digitalisierung und Industrie 4.0 zu unterstützen. Anforderungen an eine unternehmensübergreifende Dateninfrastruktur, Visibilität von Produktionsdaten im gesamten Wertschöpfungsnetzwerk und Nutzbarkeit für dezentrale Supply-Chain-Strukturen bei gleichzeitiger Gewährleistung von Datensicherheit stehen dabei im Mittelpunkt. Basierend auf der technischen Grundlage der Blockchaintechnologie (BC-Technologie) wird eine Referenzarchitektur für Blockchainapplikationen im SCM konzipiert und Anforderungen durch Anwender erarbeitet. Mit Hilfe des DIN fließen Ergebnisse in die Standardisierung ein und konkrete Anwendungsmöglichkeiten werden analysiert. Die Referenzarchitektur dient dabei der erleichterten Entwicklung und Implementierung anwendungsspezifischer Lösungen und damit einer Reduzierung von Kosten, Risiken und Zeitaufwand für KMU. Die Standardisierung kann verlässliche Rahmenbedingungen bieten sowie Unsicherheiten und Schnittstellenprobleme reduzieren. Gleichzeitig stellt sie eine notwendige Grundlage für eine effiziente Nutzung über die gesamte Supply-Chain dar. Auf der Referenzarchitektur und den Standardisierungsaktivitäten aufbauend sollen Gestaltungsempfehlungen entwickelt werden, die den Transfer der Forschungsergebnisse zusätzlich sicherstellen.

1.2 Projektplan und -verlauf

Das Projekt wurde in sechs inhaltliche Arbeitspakete (AP) unterteilt.

In AP 1 „Anforderungen an BC-Applikationen“ erfolgte eine umfassende, industrieseitige Anforderungsaufnahme. Dabei wurden die Anforderungen an eine BC-Applikation im SCM durch die üblicherweise in Logistikketten Partizipierenden berücksichtigt. Produzierende Unternehmen, Logistikdienstleister und Lösungsanbieter wurden in strukturierten Interviews befragt und die Ergebnisse in einer Anforderungsübersicht aufbereitet. Hierbei wurden insbesondere die umfassenden Netzwerke des FIR und des DIN genutzt. Beachtung fanden dabei alle relevanten Unternehmensebenen und -abteilungen; die Identifikation derselben fand zuvor mit Führungskräften der Unternehmen statt. Hierfür sollte zunächst mit strukturierten Interviews eine qualitative Analyse stattfinden. Die erfassten Anforderungen werden priorisiert und in entsprechende Kategorie eingeteilt.

Inhalt des Arbeitspakets 2 „Funktions-Referenzarchitektur BC-Applikationen“ war die Erstellung einer möglichst generischen Beschreibung von BC-Applikationen durch eine strukturierte Anordnung von Modulen, für deren einzelnen Module verschiedene spezifische Ausprägungen identifiziert wurden. Es war nicht das Ziel, eine konkrete Softwarearchitektur zu entwickeln, vielmehr eine Funktionsarchitektur. Auf Basis einer fundierten Literatur- und Marktrecherche wurden zunächst sowohl kommerziell eingesetzte als auch sich in Entwicklung befindliche BC-Applikationen untersucht und vor dem Hintergrund ihrer Anwendungsfälle jeweils in entsprechende Module unterteilt. Anschließend wurde aus den verschiedenen spezifischen Unterteilungen eine generische Unterteilung abgeleitet. Ferner erfolgte eine Festlegung verschiedener Ausprägungen, die einzelne Module entsprechend dem spezifischen Anwendungsfall häufig annehmen. Abschließend wurde daraus das Gesamtbild einer Referenzarchitektur abgeleitet; in diesem Fall eine grundsätzliche generische, modulare Struktur, für deren einzelne Module anwendungsfallsspezifische Ausprägungen aufgeführt werden.

AP 3 beinhaltete die „Identifikation von relevanten Daten und Schnittstellen“. Da eine Blockchain eine dezentrale Datenbank darstellt, ist die Identifikation relevanter Schnittstellen direkt an die Identifikation nutzenversprechender, geeigneter Daten und deren Quellen geknüpft. Hierfür wurden in diesem Arbeitspaket zunächst relevante, das SCM betreffende Unternehmensdaten identifiziert sowie strukturiert. Selbige wurden auf Kompatibilität entsprechend der Referenzarchitektur aus AP 2 dahingehend geprüft, ob diese hinsichtlich der funktionalen Perspektive adäquat verarbeitet werden können und ob spezifische Ausprägungen der Module empfehlenswert oder notwendig sind. Zudem wurde geprüft, ob eine Datenhaltung der identifizierten Daten in einer BC-Applikation geeignet ist, die in AP 1 identifizierten Anforderungen zu erfüllen. Weiterhin wurde für diese Daten festgestellt, in welchen unternehmenseigenen Quellen (bspw. ERP-System oder TMS) diese vorliegen. Die Erfassung fand unter anderem mit Vertretern des PAs und in einem

Workshop mit Unternehmen aus der Industrie statt, um Praxisrelevanz und -bezug sicherzustellen. Für die identifizierten Daten wurden entsprechende Schnittstellen betrachtet und deren Standardisierungsrelevanz bewertet.

In AP 4 „Standardisierung“ fand zunächst die Koordination der im Arbeitspaket anfallenden Aufgaben statt (AP 4.1). Daraufhin erfolgte die Normenrecherche, bei der das Normungsumfeld durchleuchtet sowie themen- und projektrelevante Normen und Standards sowohl auf nationaler als auch auf europäischer und internationaler Ebene analysiert werden (AP 4.2). Dies geschah in erster Linie durch Datenbankrecherche unter Zuhilfenahme der Datenbanken von DIN. Basierend auf den Ergebnissen vorangegangener Recherchen wurden projektrelevante Normungs- und Standardisierungsaktivitäten identifiziert (AP 4.3). Aktuelle, auf nationaler, europäischer oder internationaler Ebene laufende Normungs- und Standardisierungsaktivitäten wurden dabei hinsichtlich der Möglichkeit ihrer Berücksichtigung in den Projekten geprüft. Aus den Ergebnissen vorangegangener Recherchen und Analysen wurden projektspezifische Standardisierungsbedarfe und -potenziale innerhalb des Forschungsprojekts ermittelt (AP 4.4). Insbesondere werden die Projektpartner in die Vorgehensweise bei der Einbringung von Normungsideen in die nationale/europäische/internationale Normung eingeführt. Anschließend werden Standardisierungsarbeiten initiiert zur Erstellung eines Standardisierungsdokuments (DIN SPEC) (AP 4.5). DIN hat die Dokumentenerstellung im Unterauftrag begleitet.

Das AP 5 „Gestaltungsempfehlung zur Integration einer BC-Applikation“ befasst sich mit der Erstellung eines konkreten Gestaltungsleitfadens. Der Entwurf von Gestaltungsempfehlungen wurde umgesetzt, um eine Anwendung der Forschungsergebnisse mit minimalem Aufwand zu ermöglichen und damit Unsicherheit, Risiko sowie Initialkosten seitens der KMU bei der Integration von BC-Applikationen zusätzlich zu reduzieren. So soll das Unternehmen befähigt werden, entweder entsprechend einem konkreten Anwendungsfall vielversprechende Daten sowie deren typischen Quellen (AP 3) zu identifizieren sowie spezifische Ausprägungen der Module des Referenzmodells abzuleiten (AP 2). Aufbauend hierauf sollte das Unternehmen entweder in der Lage sein, eine entsprechende Umsetzung selbst vorzunehmen oder ein anforderungsgerechtes Lastenheft für den speziellen Anwendungsfall zu verfassen.

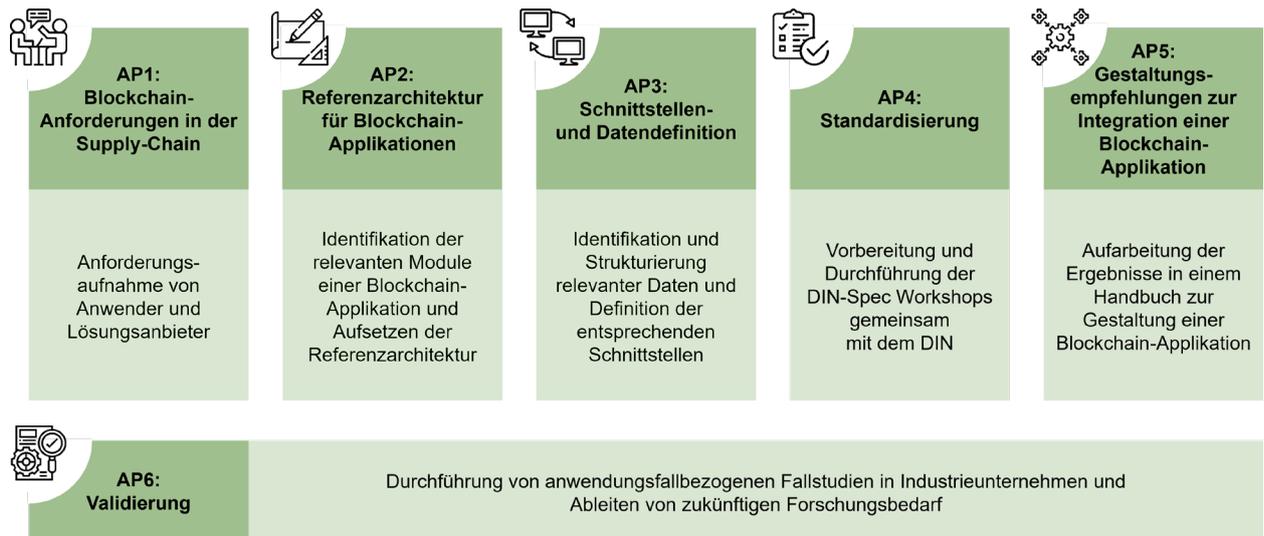


Abbildung 1: Überblick über die Arbeitspakete des Forschungsprojekts ‚ABChain‘

2 Durchgeführte Arbeiten und Ergebnisse

In den folgenden Kapiteln werden die im Forschungsvorhaben durchgeführten Arbeiten und die erzielten Ergebnisse beschrieben. Diese sind entlang der im Arbeitsplan verankerten AP strukturiert.

2.1 AP 1: Anforderungen an Blockchain-Applikationen

Arbeitspaket 1 hat zum Ziel, eine Übersicht über die bestehenden Anforderungen an eine Blockchain-Applikation seitens der beteiligten KMU zu erhalten. Darüber hinaus sollen auch die Anforderungen von Lösungsanbietern aufgenommen werden. Diese umfassen vor allem Anforderungen an die Unternehmen, Restriktionen in Bezug auf die technische Machbarkeit sowie Anforderungen, die die Unternehmen durch die Erfahrung in der Zusammenarbeit mit Kunden gesammelt haben.

Zum Start des Projekts wurden gemeinsam mit dem projektbegleitenden Ausschuss im Rahmen des Kick-off-Treffens in Aachen relevante Usecases definiert. Dazu wurden zunächst die erforderlichen Grundlagen wissenschaftlich und literaturbasiert vorbereitet. Zur Aufnahme der Anforderungen in strukturierten Interviews wurden zunächst Interviewleitfäden für die verschiedenen Zielgruppen der Anwender, Lösungsanbieter sowie spezifischen Expert:innen erstellt. Im Nachgang wurden Interviews mit insgesamt 13 Partnern aus Industrie und Wissenschaft durchgeführt. Nach der Transkription der Interviews wurden die zentralen Aussagen identifiziert und konsolidiert, sodass in einem gemeinsamen Workshop die Priorisierung der Anforderungen stattfinden konnte.

Da die Nachverfolgung von Nachhaltigkeitskriterien als ein relevanter Usecase identifiziert wurde, wurde darüber hinaus auch eine Online-Umfrage mit Endverbrauchern durchgeführt, um die Relevanz der Informationen sowie die Anforderungen an eine Informationsbereitstellung zu identifizieren. Die Ergebnisse zur Anforderungsaufnahme mit den Interviewpartner:innen der Unternehmen wurden im Magazin „Logistik Heute“ veröffentlicht. Für die Ergebnisse aus der Online-Umfrage ist eine Veröffentlichung in Q1/2023 geplant.

Bei der Erstellung der Interviewleitfäden wurden für die verschiedenen Stakeholder (bspw. Anwender:innen, Expert:innen für Datenschutz, Anbieter:innen) unterschiedliche Interviewleitfäden erstellt. Untenstehend ist exemplarisch der Interviewleitfaden für potenzielle Anwender:innen einer Blockchain-Applikation aufgeführt.

Interviewfragen Anwender:innen
Einstieg
<p>1. Inwieweit haben Sie sich bereits mit dem Thema Blockchain-Applikationen im Supply-Chain-Management auseinandergesetzt? Und wie vertraut sind Sie mit der Blockchain-Technologie? <i>Kurze Erklärung von dem BC und der Anwendung des überbetrieblichen Datenaustauschs – auf das vorher Gesagte eingehen und fehlende Punkte ergänzen, sodass ein gleiches Grundverständnis herrscht:</i></p> <ul style="list-style-type: none"> ○ <i>Blockchain als verteilte und fälschungssichere Datenbank</i> ○ <i>Einfacher überbetrieblicher Zugriff auf die Daten</i> ○ <i>Kryptografische Hash-Funktionen, die Informationen verschlüsseln, sodass diese nur mit dem entsprechenden Schlüssel gelesen werden können</i> ○ <i>Verifizierung der Informationen durch den persönlichen Schlüssel des Absenders</i> ○ <i>Einmal geteilte Informationen können nachträglich nicht verändert werden</i> ○ <i>Sicherheit gegen Datenverlust durch dezentrale Speicherung – hoher Ressourcenverbrauch durch benötigte Serverkapazitäten</i> ○ <i>Lokale Verfügbarkeit der Daten durch dezentrale Speicherung</i> ○ <i>Arbeiten ohne zusätzlichen Intermediär wie Cloud-Provider möglich</i> ○ <i>Überbetrieblicher Datenaustausch, um besser auf Veränderungen in der Lieferkette eingehen zu können (z. B. Kenntnisse über Produktionsverzögerungen bei Lieferanten)</i> ○ <i>Informationen zur Nachhaltigkeit der eigenen und der Zulieferer-Unternehmensprozesse können geteilt werden</i>
Themenkomplex I: Anforderungen
<p>2. Welche Anforderungen müsste eine Blockchain-Applikation für Sie erfüllen, damit Sie sie im Unternehmen einführen und nutzen würden?</p> <ul style="list-style-type: none"> ○ Datensicherheit ○ Benutzeroberfläche ○ Schnittstellen ○ Dokumentation welcher Prozesse ○ Kosten und Aufwand (Bereitstellung Serverkapazitäten, Investitionskosten, Schulung, automatisches Abgreifen der Informationen aus einem bestehenden System oder manuelles Nachpflegen) ○ Nutzerkreis
Themenkomplex II: Daten/Datensicherheit
<p>3. Unter welcher Voraussetzung wären Sie bereit, Daten entlang der Wertschöpfungskette zu teilen?</p> <ul style="list-style-type: none"> ○ <i>Gibt es bestimmte Daten, die Sie nicht teilen würden? (Verarbeitungsschritte, Standortinformationen, Prozessfortschritt, Arbeitsbedingungen, Betriebsorganisation, Verbrauchsdaten etc.)</i> ○ <i>Wenn ja, woran liegt das?</i> <p>4. Wie sollten Ihrer Meinung nach die Zugriffsrechte innerhalb der Blockchain verteilt sein?</p> <p>5. <i>Angenommen, Sie würden alle Informationen zu z. B. Verarbeitungsschritten, Standortinformationen, Prozessfortschritt, Arbeitsbedingungen, Betriebsorganisation, Verbrauchsdaten in einer Blockchain ablegen, hätten Sie das Gefühl, die Daten wären sicher? Auch vor kryptografischen Angriffen? (Wenn nein, wieso nicht?)</i></p>
Themenkomplex III: Nachhaltigkeitskriterien
<p>6. Wie hoch schätzen Sie die Relevanz von der Rückverfolgbarkeit von Nachhaltigkeitskriterien über die Lieferkette in Ihrem Unternehmen ein?</p> <p>7. Wie müssen die Daten bereitgestellt oder verifiziert werden, damit Sie diese als echt anerkennen?</p>

Abschluss
8. Angenommen, Sie arbeiten in Ihrem gesamten Wertschöpfungsnetzwerk in einer Blockchain-Applikation, um Daten zu teilen, Sie erhalten so auch die Informationen von den Zulieferern Ihrer Zulieferer usw. Wo sehen Sie die größten Vorteile und Herausforderungen?
9. <i>Wo sehen Sie noch weitere Anwendungsfälle von Blockchain-Applikationen?</i>
10. <i>Welche negativen Aspekte, im gesamten Projektzeitraum, würden für Sie den direkten Projektausstieg bedeuten?</i>

Tabelle 1: Interviewleitfaden

Nach der Durchführung der Interviews mit insgesamt 21 Partner:innen wurden die Interviews transkribiert und ausgewertet. Dazu wurden zunächst die Aussagen der Teilnehmenden vereinheitlicht und anschließend geclustert. So konnten Anforderungen in 21 unterschiedlichen Kategorien identifiziert und klassifiziert werden. Die häufigsten Anforderungen können Abbildung 2-1 entnommen werden. Eine zentrale Anforderung durch alle Anwendenden war die nahtlose Integration der Blockchain-Lösung in die bestehenden IT-Systeme. Hierbei sollte stets die Möglichkeit zur Unterscheidung zwischen relevanten und irrelevanten Daten für das Teilen entlang der Lieferkette gegeben werden. Eine große Rolle spielte auch die Datensicherheit und der Zugriff auf die Daten durch Partner:innen sowie Dritte. Neben der Umsetzung von Informationssicherheit und der DSGVO war es den produzierenden Anwender:innen insbesondere 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, soll sehr präzise ermöglicht werden. Bei den Logistikdienstleistern lag dies nicht im Fokus, da größtenteils durch deren Kund:innen gesteuert wird, wer die Daten einsehen kann, und die Datenhoheit nicht bei ihnen selbst liegt. Diese Sicherheitsanforderungen können technologisch über die Schlüssel-paare in der Blockchain sowie die redundante Datenhaltung erfüllt werden. Im Rahmen der Gestaltung der Zugriffsrechte war auch die Governance der Blockchain-Applikationen ein wichtiges Thema. Hierbei gilt es, diejenigen Unternehmen und Richtlinien zu bestimmen, die im Zweifelsfall über die Gültigkeit von Daten und Transaktionen entscheiden können. Dieses Thema wird auch im weiteren Projektverlauf genauer betrachtet.

Im Nachgang zu den Interviews wurde im Rahmen eines Projekttreffens eine zusätzliche Priorisierung der Anforderungen vorgenommen. Diese Priorisierung ist auch in die wesentlichen Anforderungen in Abbildung 2-1 eingeflossen.

herausgestellt, da diese insbesondere bei Bio- oder fair hergestellten Rohstoffen beziehungsweise Produkten eine große Rolle spielen. Neben den Anwendungsfällen im Bereich der Nachhaltigkeit wurde außerdem die Abwicklung von Zahlungen bei Lieferungen, insbesondere bei Schüttgut oder aber eine Rückverfolgung sicherheits-relevanter Bauteile von Produkten aufgeworfen. Die generelle Transparenz in der Supply-Chain, die die Einführung einer solchen Lösung schafft, ermöglicht jedoch noch weitere Anwendungsfälle zur Optimierung und Verbesserung der überbetrieblichen Prozesse. Die identifizierten Anwendungsfälle können auch Abbildung 2-2 entnommen werden.

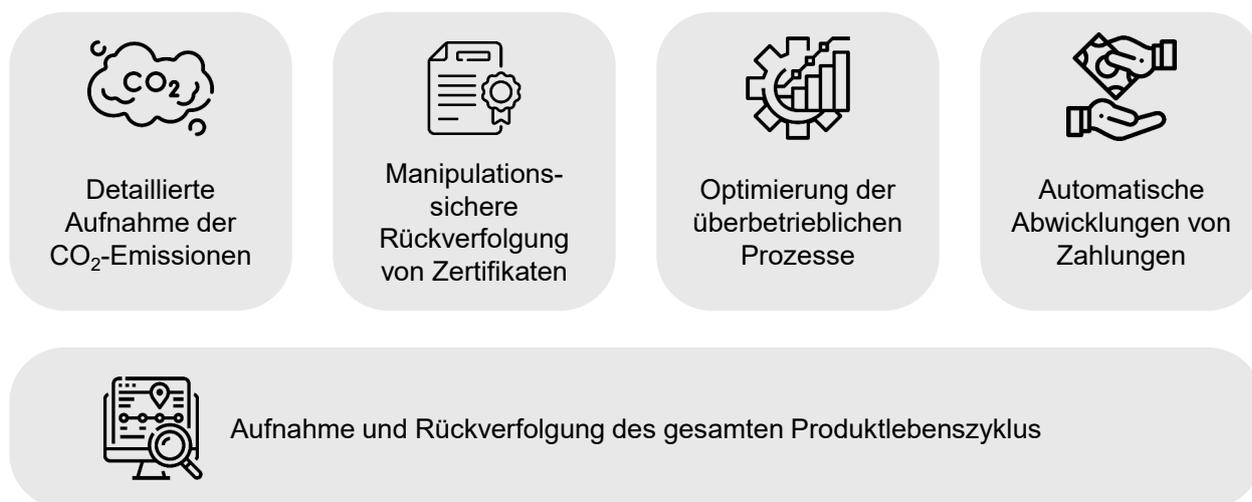


Abbildung 3: Anwendungsfälle für den Einsatz einer Blockchain-Applikation im SCM

Das Ziel von AP 1, eine aus strukturierten Interviews resultierende Anforderungsübersicht seitens KMU an die Blockchain-Applikation zu erstellen, wurde erfolgreich im Projekt erarbeitet. Der dabei entstandene, exemplarische Interviewleitfaden für potenzielle Anwender:innen einer Blockchain-Applikation dient zur Identifizierung und Klassifizierung zahlreicher Anforderungen in unterschiedlichen Kategorien. Außerdem wurden, basierend auf den durchgeführten Interviews, potenzielle Anwendungsfälle für eine Blockchain-Applikation im Supply-Chain-Management (SCM) ausgedrückt. Die dabei entstandene Abbildung identifiziert die beschriebenen Anwendungsfälle.

2.2 AP 2: Blockchain-Referenzarchitektur

Arbeitspaket 2 hat zum Ziel, ein grundlegendes Verständnis für Blockchains und deren Funktionsweise zu schaffen, indem die einzelnen Merkmale der Blockchain-Technologie in ihren Ausprägungen näher erläutert werden. Der daraus resultierende morphologische Kasten im Sinne einer Referenzarchitektur für Blockchain-Applikationen soll die Entscheidung zwischen einer Vielzahl von Applikationen für die Anwender und Anbieter ermöglichen.

Die Blockchain-Technologie, oder auch DLTs im Gesamten, kann durch ihre breiten Variationen in verschiedensten Themenfeldern genutzt werden (s. BERGHOFF ET AL. 2019, S. 10–11). Blockchainbasierte Systeme und Applikationen unterliegen dadurch der Schwierigkeit, dass sich in der Entwicklung zwischen einer Vielzahl an Konfigurationen entschieden werden muss. Nach einer Erläuterung der Grundlagen der Blockchain-Technologie wird im Folgenden in Anlehnung an HOLTKEMPER (2020, S. 126) ein Überblick über die morphologischen Merkmale und ihre möglichen Ausprägungen gegeben, sodass sich im Gesamten eine Morphologie der Blockchain-Technologie ergibt.

2.2.1 Grundlagen

Dieses Kapitel zielt auf ein einheitliches Verständnis bzgl. der Blockchain-Technologie ab und bildet die Voraussetzung für die weiteren Ausführungen. Aufgrund dessen werden einleitend die Funktionsweisen der Blockchain erläutert.

FUßWINKEL U. KREITERLING beschreiben Blockchains als fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind (s. FUßWINKEL U. KREITERLING 2019, S. 9f.). Diese benannten Eigenschaften resultieren aus verschiedenen technologischen Verfahren. Technologisch gesehen setzt sich die Blockchain aus einzelnen Blöcken zusammen, die als Kette manipulations-sicher miteinander verknüpft sind. Somit werden neu aufgenommene Daten, die die Inhalte der Blöcke darstellen, kryptographisch verschlüsselt und mit einem individuellen Hash versehen, ans Ende der Kette gefügt.

Die Verfügbarkeit der Blockchain geht aus der Speicherung auf den Rechnern eines verteilten Peer-to-Peer(P2P)-Netzwerks hervor. Die einzelnen Rechner stellen nach dieser Grundlage einzelne Knoten dar, die die Ressourcen wie beispielsweise die Speicherkapazität, Rechenleistung oder Daten bereithalten. Diese Netzwerkknoten administrieren jeweils eine Kopie der gesamten Daten der Blockchain und können neue Daten hinzufügen. Die Aktualität sowie die Übereinstimmung der Daten innerhalb der einzelnen Knoten ist durch einen geeigneten Konsensmechanismus gesichert (s. BERGHOFF ET AL. 2019, S. 9).

Technologisch geeignet ist die Blockchain somit insbesondere aus Gründen des Datenschutzes. Dies basiert nach SCHLATT ET AL. auf der Nutzung der Hash-Funktionen in einer Blockchain, die eine Veränderung der Daten aus Manipulationsgründen ausschließt. Die Basis der Blockchain besteht aus den zuvor aufgeführten kryptografischen Hashfunktionen, welche die Informationen in eine Zeichenfolge fixer Länge umwandeln, den Hashwert. Dabei ergeben dieselben Informationen immer denselben Hashwert. Bereits leicht veränderte Funktionen ergeben jedoch einen stark abweichenden Hashwert, während der Hashwert selbst keine Informationen preisgibt. (s.

SCHLATT ET AL. 2016, S. 8; s. BADEV U. CHEN 2014, S. 9) Unterstützend, zur Vermeidung von Manipulation und zur Garantie der Authentizität der Informationen dient die Nutzung eines mathematischen Schlüsselpaars. Der Versender hat die Möglichkeit, seine Information mit seinem persönlichen Schlüssel zu signieren, sodass der ausgewählte Empfänger diese nur mit dem dazugehörigen Schlüssel öffnen kann. (s. SCHLATT ET AL. 2016, S. 8) Eine dezentrale Speicherung der Daten gewährleistet zum einen die Sicherheit gegen den Datenverlust und impliziert zum anderen, dass alle beteiligten Stakeholder die Daten lokal zur Verfügung gestellt bekommen und somit jederzeit darauf zugreifen können (s. SIEGEL 2017, S. 45).

Resultierend ist die rein technologische Eignung der Blockchain im Supply-Chain Management gegeben. Um die Leistungsfähigkeit der Blockchain auszuschöpfen, soll eine anwendungsspezifische Blockchain-Architektur, die die Anforderungen der Anwender und Anbieter berücksichtigt, die sogenannte AB-Chain, genutzt werden.

Merkmal	Ausprägung			
Grad der Datenverteilung	Vollständige Daten je Knoten	Knoten mit und ohne vollständige Daten		Vollständige Daten nur bei zentralem Knoten
Abzuspeichernde Daten	Transaktionen	Code	Dateien	Hash-Werte
Informationsfreigabe	Keine Begrenzung	Für Adressat der Transaktion und alle Folgenden	Für Adressat der Transaktion	Individuell
Lesezugang	Genehmigungsfrei		Genehmigungspflichtig	
Schreibzugang	Genehmigungsfrei		Genehmigungspflichtig	
Regelwerk zur Datenaufnahme	Nur nach Datenstruktur	Regelwerk nach Knoten	Plausibilitätsprüfung	(Regelwerk auf Server)
Anreizmechanismus	Handelbare Coins	Intrinsisch		Vertragliche Regelungen
Datenablage	On-Chain		On- und Off-Chain	
Bekanntheit der Teilnehmenden	Teilnehmende bekannt	Pseudonymität		Anonymität
Konsensalgorithmus	Proof of Work (PoW)	Proof of Stake (PoS)	Practical Byzantine Fault Tolerance Algorithm (PBFT)	Proof of Elapsed-Time (PoET)

Abbildung 4: Morphologie der Blockchain-Technologie

Die einzelnen Merkmale und ihre Ausprägungen werden im Folgenden erläutert.

2.2.2 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. die Menge und Vollständigkeit der Daten sowie die Anzahl der Knoten. Sowohl das Schreiben als auch das 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 (s. HOLTKEMPER 2020, S. 90):** Bei vollständigen Daten je Knoten besteht eine hohe Verfügbarkeit von Daten innerhalb der Blockchain sowie ein hoher Schutz vor Datenverlust und Manipulation. Alle Knoten sind sog. Full-Nodes.
- **Knoten mit und ohne vollständige Daten/Selective Nodes (s. HOLTKEMPER 2020, S. 91):** „Lightweight-Nodes“ speichern nur den für den Besitzer des Knotens relevanten Teil der Blockchain. Lightweight-Nodes sind bei der Verifizierung auf Full-Nodes angewiesen, die Datenmenge im Blockchain-Netzwerk wird somit reduziert.
- **Vollständige Daten nur bei zentralem Knoten (s. HOLTKEMPER 2020, S. 92):** Es besteht eine zentralisierte Datenstruktur, d. h. es existiert eine Full-Node (z. B. ein zentrales Unternehmen) und sonst nur Light-Nodes, die auf das eine Unternehmen angewiesen sind. So liegt im Vergleich zu vollständigen Knoten im gesamten dezentralen Netzwerk nur eine sehr geringe Datenmenge vor.

Die 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 Optimierungsansätze: Schnelligkeit beim Zugriff steht einer hohen Datenverfügbarkeit entgegen. Genauso ist der Schutz von Daten häufig verzögert. Aus diesen Gründen wird eine frühe umfassende konzeptionelle Auseinandersetzung über die vielfältigen Optionen empfohlen. Spätere Anpassungen bei Datenverteilung und -zugriff sind dagegen sehr aufwendig und teuer. Insbesondere gilt dies für die Anlage von Smart Contracts.



Abbildung 5: Grad der Datenverteilung

2.2.3 Abzuspeichernde Daten

Welche Daten aus Supply-Chains auf einer Blockchain gespeichert werden sollen, spielt eine zentrale Rolle für Nutzbarkeit und Kosten. Limitierend wirkt dabei besonders die Größe der Daten

und somit die Performance. Aber auch eine klare Struktur (Format: vereinbarte Syntax und Semantik) der Daten, die ihre Relevanz für deren Nutzer widerspiegelt, sind von Bedeutung für die Informationsgewinnung durch die Supply-Chain-Teilnehmenden.

- **Transaktionen:** Eine Transaktion ist eine Operation, die einen neuen Zustand der Datenbank definiert (s. WUST; GERVAIS 2018, S. 1), beispielsweise ein Kaufvertrag oder die Zertifizierung für ein Gut.
- **Hashwerte:** Ein Hashwert ist die Verschlüsselung eines Datensatzes (s. HOLTKEMPER 2020, S. 26) und 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, da der Hashwert sich mit Ändern der Daten/Dokumente auch ändert. Der Inhalt der Daten/Dokumente kann jedoch nicht überprüft werden, sodass jener bei einer zentralen Datenhaltung abseits der Blockchain gelöscht und abgestritten werden kann (s. HOLTKEMPER 2020, S. 156). Es kann lediglich nachgewiesen werden, dass eine Änderung stattgefunden hat. (s. HOLTKEMPER 2020, S. 27) Die Daten selbst sind nicht auf der Blockchain abgelegt. Die Hashwerte haben eine vergleichsweise sehr geringe Größe (s. FRANCO 2014, S. 96).
- **Code:** Über den Code ist eine Implementierung von sog. Smart Contracts möglich (s. HOLTKEMPER 2020, S. 95) sowie Darstellungen von Wenn-dann-Beziehungen (s. HOLTKEMPER 2020, S. 95). Der Code hat vergleichsweise eine mittlere Größe, die je nach Gestaltung variiert.
- **Dateien:** Es besteht die Möglichkeit, komplette Dateien auf der Blockchain abzuspeichern (s. HOLTKEMPER 2020, S. 96), darunter fallen beispielsweise Textdateien, Audiodateien, oder Bilddateien und Zertifikate (s. FISCHER U. HOFER 2011, S. 206). Diese Daten sind vergleichsweise sehr groß (s. HOLTKEMPER 2020, S. 96).

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 Open-Source-Lösungen als Grundlagen dienen.

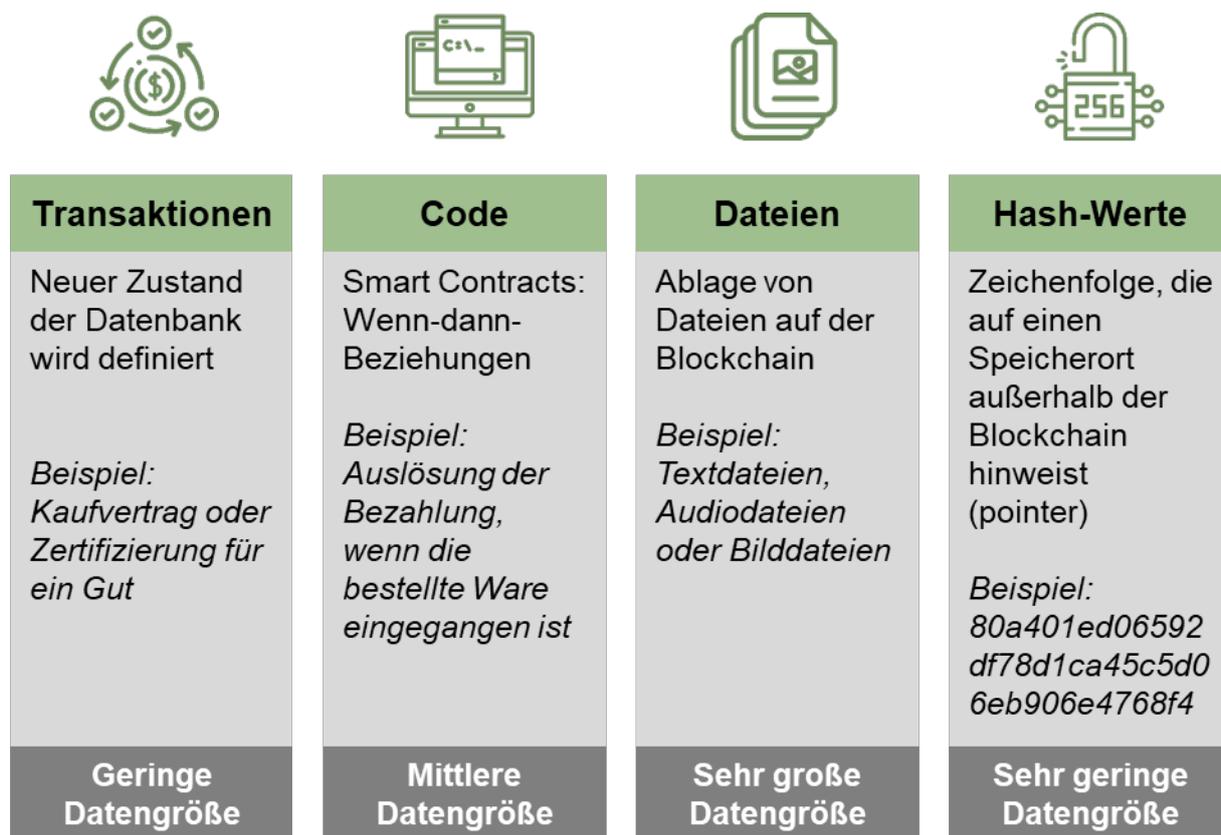


Abbildung 6: Abzuspeichernde Daten

2.2.4 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 (s. HOLTKEMPER 2020, S. 98).
- **Für Adressat der Transaktion und alle Folgenden:** Der Inhalt der Transaktion ist nur für den Empfänger sowie alle folgenden Teilnehmenden bekannt (s. GAO ET AL. 2018, S. 244). Soll im Sinne des Schutzes von bspw. Geschäftsgeheimnissen verhindert werden, dass nicht alle nachfolgenden Teilnehmenden alle Informationen erhalten, ist ein Rechtemanagement-System notwendig (s. HOLTKEMPER 2020, S. 99).

- **Für Adressat der Transaktion:** Das Ziel ist der Austausch von Informationen zwischen genau zwei Teilnehmenden (s. GAO ET AL. 2018, S. 244). Eine Verschlüsselung durch den Private-Key des Adressaten ist möglich (s. GAO ET AL. 2018, S. 244). Die Reproduktion der Information kann nicht verhindert werden (dies ist ein grundsätzliches Problem und nicht spezifisch für die Blockchain-Technologie) (s. HOLTKEMPER 2020, S. 100).
- **Individuelle Informationsfreigabe:** Sonderfälle können individuelle Anforderungen darstellen (s. HOLTKEMPER 2020, S. 101). Die Verschlüsselung jeder Information und anschließende Schlüsselverteilung an betreffende Teilnehmende stellt einen solchen Sonderfall dar (s. HOLTKEMPER 2020, S. 101). Digitale Identitäten ermöglichen neben einer individuellen Verteilung auch die Verteilung an Gruppen.



Abbildung 7: Informationsfreigabe

Im Sinne der kollaborativen Informationsgewinnung für Supply-Chain-Partner 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 versus 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 Informationsaustausch unter Partner:innen, die sich kennen, oder anonymen Supply-Chain-Teilnehmenden, die sich noch nicht begegnet sind, kann durch Zuhilfenahme von digitalen Identitäten, i. d. R. zentral oder dezentral ausgeblendet werden.



Abbildung 8: Informationsfreigabe

2.2.5 Lese- und Schreibzugang

Supply-Chain-Partner:innen können sich auf die gemeinsame Datennutzung in Blockchains einigen. Dazu sind ihr Lese- und Schreibzugang 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 dazugehörigen Datenökosystems 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:

- **Genehmigungsfrei:** Lese- und Schreibzugang sind genehmigungsfrei (s. WUST U. GERVAIS 2018, S. 1).
- **Genehmigungspflichtig:** Der Lese- und Schreibzugang ist genehmigungspflichtig (s. GARZIK 2015, S. 10). 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-Algorithms verwendet werden können (wenn schädliches Handeln durch autorisierte Teilnehmende ausgeschlossen wird). Für eine Erläuterung der Algorithmen siehe Kap. 5.1.9 (s. HOLTKEMPER 2020, S. 104). Eine (zentrale) Instanz unterhält dabei die Blockchain (s. WUST U. GERVAIS 2018, S. 1).

2.2.6 Regelwerk zur Datenaufnahme

Bevor Transaktionen an benachbarte Knoten weitergeleitet werden, sind die Daten nach den im Blockchain-Protokoll festgelegten Kriterien zu überprüfen (s. FRANCO 2014, S. 110).

- **Nur nach Datenstruktur:** Die Formatierung der Daten ist zu verifizieren (s. HECKEN 2016, S. 527). Überprüft wird dabei beispielsweise, ob die Syntax und das Format der Daten den Vorgaben entsprechen. Weiterhin dürfen die Inputs oder Outputs der Transaktion nicht null sein und eine Transaktion darf nur eine begrenzte Anzahl von Token übertragen (s. HOLTKEMPER 2020, S. 107).
- **Regelwerk nach Knoten:** Das Regelwerk wird durch Summenbildung auf die Konsistenz von Wert- oder Zahlenangaben nach Knoten überprüft (s. HOLTKEMPER 2020, S. 107). So ist beispielsweise eine neue Transaktion erlaubt, wenn die ermittelte Summe der Transaktionsbetrachtung (Inputs und Outputs) größer ist als die Summe der neuen Transaktion.
- **Plausibilitätsprüfung:** Eine Plausibilitätsprüfung meint die Kontrolle der Daten hinsichtlich ihrer Plausibilität (s. HECKEN 2016, S. 527). Dabei finden beispielsweise eine vorgelegte Überprüfung der Datenstruktur sowie eine Eingrenzung der Gesamtmenge von Tokens statt, die in einem festgelegten Zeitintervall transferiert werden dürfen (s. HOLTKEMPER 2020, S. 108). Ein genauer Regelkatalog muss festgelegt werden.

2.2.7 Anreizmechanismen

Anreizmechanismen sollen die Partner:innen einer Supply-Chain dazu motivieren, die Blockchain zu nutzen, um einen größtmöglichen Nutzen zu erzielen. Die Anreize für die teilnehmenden Unternehmen können unterschiedlicher Natur sein und haben nur in der Ausprägung der handelbaren Coins einen Einfluss auf die tatsächliche Ausgestaltung der Blockchain-Anwendung.

- **Handelbare Coins:** Handelbare Coins stellen eine virtuelle „Währung“ zur Belohnung bzw. Bezahlung innerhalb des Netzwerks dar (s. SORGE U. KROHN-GRIMBERGHE 2013, S. 720).
- **Intrinsisch:** Die Teilnehmenden nutzen die Blockchain aus eigenem Interesse (bspw. Marktmacht etc.) (s. HOLTKEMPER 2020, S. 123).
- **Vertraglich:** Die Teilnehmenden im Netzwerk sind an bestimmte Vorgaben vertraglich gebunden (bspw. Vorgaben durch Kundenverträge etc.) (s. Walport 2016, S. 44).

2.2.8 Datenablage

Wo werden die Daten gespeichert? On-Chain: Die Daten selbst liegen auf der Blockchain (s. BERGHOFF ET AL. 2019, S. 31). Off-Chain: Ein Pointer (Hashwert der Daten) wird immer abgelegt, die Daten selbst sind an einem anderen Ort gespeichert (s. BERGHOFF ET AL. 2019, S. 31).

- **Ausschließlich On-Chain:** Auf der Blockchain liegen hohe Datenmengen und hohe Kosten vor (s. HEPP ET AL. 2018, S. 284), die durch die Blockchain kryptografisch abgesichert sind und deren Zentralisierungsgrad niedrig ist.
- **Off-Chain mit zentraler Datenablage:** Die Datenmenge auf der Blockchain ist vergleichsweise gering und dadurch besser skalierbar (s. HEPP ET AL. 2018, S. 286–287). Der Single-Point-of-Failure ist die zentrale Datenablage, die einige Vorteile eines DLT wie die hohe Verfügbarkeit und die Sicherheit vor Datenverlust aufhebt (s. HEPP ET AL. 2018, S. 286). Die Zugriffsrechte werden verteilt und der Zentralisierungsgrad ist hoch (eine zentrale Partei ist für die Off-Chain-Daten zuständig).
- **Off-Chain mit verteilter Datenablage:** Die Datenmenge auf der Blockchain ist vergleichsweise gering, wodurch eine bessere Skalierbarkeit erreicht werden kann (s. HEPP ET AL. 2018, S. 286–287). Die Datenablage hat die Hochverfügbarkeit eines verteilten Systems wie die Blockchain. Die Verschlüsselung der Daten bei der Ablage kann für Zugriffskontrolle notwendig sein (Daten liegen auch bei Teilnehmenden ab, die die Daten nicht einsehen sollten).

2.2.9 Bekanntheit der Teilnehmenden

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

- **Teilnehmende bekannt:** Jeder Teilnehmende ist bekannt.
- **Pseudonymität:** Die „Adresse“ bzw. der öffentliche Schlüssel ist grundsätzlich geschützt, allerdings kann jeder eine feste „Adresse“ im Netzwerk ein Profil erstellen.
- **Anonymität:** Die komplette Anonymität des Senders und Empfängers wird beispielsweise durch Mixing (mehrere Transaktionen, aber nur eine ist die „richtige“) oder ZK-Beweise (*Zero Knowledge*) (s. MEIER 2020, S. 351) sichergestellt.

2.2.10 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. Beispiele:

- **Proof of Work (PoW):** Die Blockerzeugung ist mit erheblichem Rechen- und Energieaufwand verbunden (s. HÄDER 2019, S. 245). Die Rechengeschwindigkeit bestimmt die Wahrscheinlichkeit, einen neuen Block zu erzeugen.
- **Proof of Stake (PoS):** PoS ist die energieeffiziente Alternative zum PoW. Der Besitz der jeweiligen Währung bestimmt dabei die Wahrscheinlichkeit, einen neuen Block zu erzeugen. (s. HOLTKEMPER 2020, S. 113)
- **Proof of Authority (PoA):** Nur bestimmte Knoten (Validatoren) können entsprechend ihrer Reputation den Konsens bilden (s. TASCA U. TESSONE 2017, S. 13). PoA gilt als robuster gegenüber PoS und findet häufig Verwendung in Smart Contracts.
- **Practical Byzantine Fault Tolerance Algorithm (PBFT):** Die Konsistenz ist gewährleistet, solange mehr als zwei Drittel der Knoten im Sinne des Netzwerks arbeiten. Der Nachrichtenaustausch zwischen Knoten gewährleistet die Konsistenz (s. HAMADI 2017, S. 85).
- **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 (s. SHAH ET AL. 2021, S. 360).
- **Proof-of-Elapsed-Time (PoET):** Die *Intel Software Guard Extension* generiert für jeden Knoten eine Wartezeit (s. HOLTKEMPER 2020, S. 117). Der Netzwerkknoten mit der kürzesten Wartezeit gilt dabei als Gewinner und darf den nächsten Block erzeugen (s. HAMADI 2017, S. 84).

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 vertrauenswürdiger Validatoren überlassen wird. Auch kann es in bestimmten Anwendungsfällen genügen, wenn die Interessenvertreter:innen 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-Transaktionen relevant sind. 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.

Resultierend ist die rein technologische Eignung der Blockchain im Supply-Chain-Management gegeben. Um die Leistungsfähigkeit der Blockchain auszuschöpfen, soll eine anwendungsspezifische Blockchain-Architektur, die die Anforderungen der Anwender und Anbieter berücksichtigt, die sogenannte AB-Chain, genutzt werden.

Das Ziel von AP 2, mittels Literaturrecherche und Marktanalyse Konzepte und entsprechende Ansprüche für Schnittstellen ausgewählter Daten zu identifizieren, wurde erfolgreich im Projekt erreicht. Die dabei entstandene Morphologie der Blockchain-Technologie spiegelt eine anwendungsspezifische Blockchain-Architektur und somit die Leistungsfähigkeit der Blockchain wider, die die Anforderungen der Anwender und Anbieter berücksichtigt, die sogenannte AB-Chain.

2.3 AP 3: Identifikation von Daten und Schnittstellen

Arbeitspaket 3 hat zum Ziel, die in der Lieferkette für den Austausch über Blockchain-Applikationen bedeutsamen Datenkategorien herauszuarbeiten und zu beschreiben. Weiterhin sollen Anforderungen an Schnittstellen und Interaktionen zu anderen IT-Systemen für ein erfolgreiches Supply-Chain-Management definiert werden.

2.3.1 Relevante Daten zum Austausch in der Lieferkette

Die zur Identifikation der im Unternehmenskontext dienden Daten wurden zum einen innerhalb des Projektkonsortiums im Rahmen eines Projekttreffens und zum anderen in einem Workshop mit externen Teilnehmenden gesammelt. Die gesammelten Punkte wurden im Anschluss geclustert und konnten dadurch in vier Kategorien gefasst werden.

Im Zusammenhang mit den „Emissionen“ eines Produkts wurden beispielsweise der CO₂-Verbrauch, der Energieverbrauch oder auch die Emissionen je Produkt und Charge im generellen genannt.

„Identifikation“ bezieht sich besonders auf die eindeutige Zuordnung von Objekten im BC-Netzwerk. Dies könnte einerseits über eine Chargennummer für Assets stattfinden, andererseits müssen jedoch auch Personen einer digitalen Identität zugeordnet werden.

Neben Emissionen sind im Bereich der Nachhaltigkeit auch „Zeugnisse und Zertifikate“ von großer Relevanz. Dies können Zeugnisse über die Authentizität von (Teil-)Produkten, aber auch Pfandnachweise sein. Außerdem sind Zertifikate über Lieferanten gegebenenfalls für das Lieferkettengesetz relevant.

Die „Produkteigenschaften“ fassen diverse Punkte zusammen. Darunter fallen zum Beispiel Materialspezifikationen, Produktdaten für ein besseres Recycling, Geodaten, Rezepturen und Inhaltsstoffe von Produkten, Temperaturdaten und noch viele mehr.

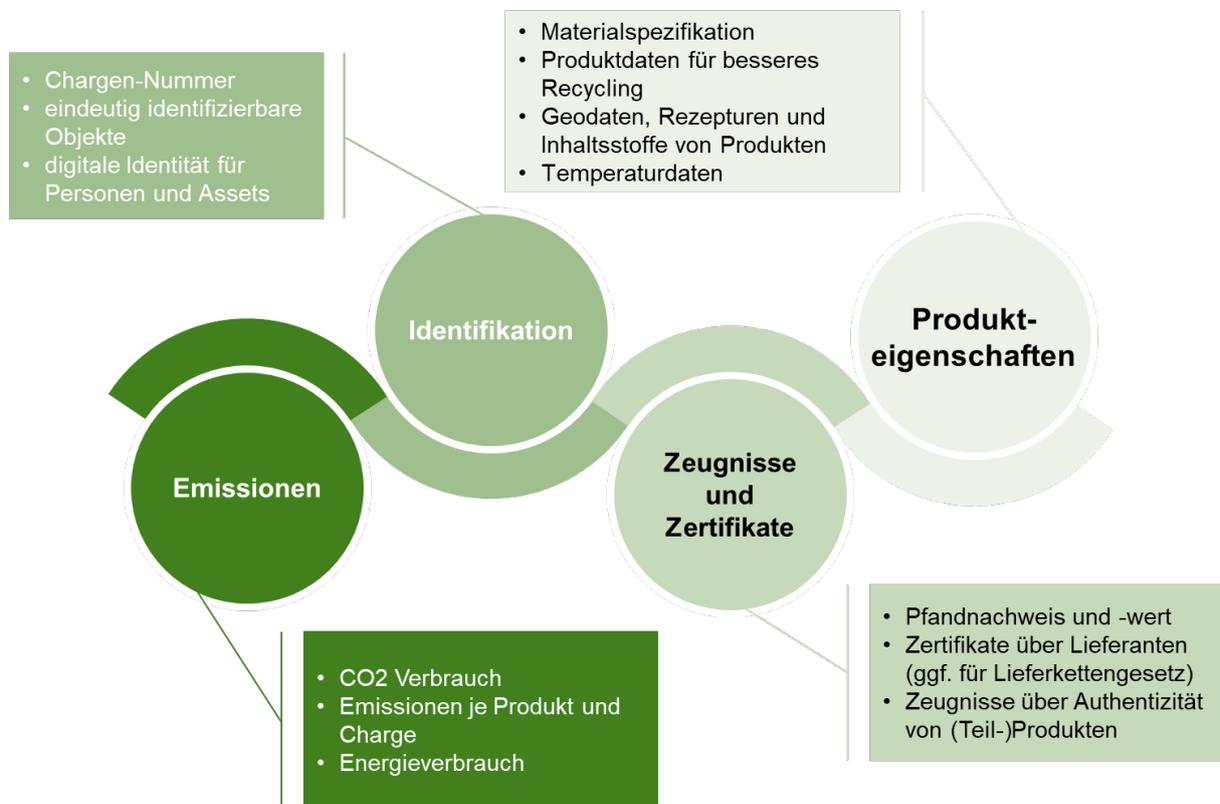


Abbildung 9: Relevante Daten, die über eine Blockchain-Applikation geteilt werden

2.3.2 Schnittstellen und Interaktion mit anderen IT-Systemen

Für die nahtlose Integration und eine sinnvolle Nutzung der Blockchain-Applikation wurde, in den Interviews für die Anforderungsaufnahme sowie in den Workshops zur Identifikation von Daten und Schnittstellen, auch die benötigte Integration in andere IT-Systeme abgefragt. Dabei war es den anwendenden Personen insbesondere wichtig, dass der Aufwand im Tagesgeschäft so gering wie möglich ist.

Für alle Befragten ist eine Schnittstelle der Blockchain-Anwendung zu den bestehenden Management-Systemen eine notwendige Voraussetzung. Mit den entsprechenden Schnittstellen soll verhindert werden, dass Daten doppelt erfasst werden müssen, um den Aufwand nicht zu erhöhen und Fehlerquellen zu vermeiden. Die Befragten sehen außerdem eine große Gefahr darin, dass eine notwendige doppelte Erfassung dazu führt, dass weniger Unternehmen die Blockchain-Applikation verwenden, wenn der Aufwand zu hoch ist. Darüber hinaus soll zudem die manuelle Eingabe von Daten ermöglicht werden, sodass auch Unternehmen partizipieren können, die die notwendigen Daten nicht in bereits bestehenden IT-Systemen erfassen und über Schnittstellen übergeben können.

Das Ziel von AP 3, die Erstellung einer modularen Referenzarchitektur für Blockchain-Applikationen im Supply-Chain-Management, wurde erfolgreich im Projekt erarbeitet. Die dabei entstandene Abbildung schildert die relevanten Daten, die über eine Blockchain-Applikation geteilt werden.

2.4 AP 4: Standardisierung in einer DIN SPEC

Arbeitspaket 4 hat zum Ziel, die Anforderungen und Merkmale einer Blockchain im Supply-Chain-Management vertieft auszuführen und mit Fallbeispielen zu ergänzen. Die ausgehend von einer Normrecherche entwickelte DIN SPEC soll dafür als Grundlage dienen. Anschließend soll die in AP 2 entwickelte Morphologie angepasst und erweitert werden.

Basierend auf den vorherigen Arbeitspaketen hat eine Normrecherche stattgefunden. Die nachfolgende Tabelle zeigt einen Auszug aus dem erarbeiteten Überblick über existierende Standards, Normen und laufenden Aktivitäten in Bezug auf dieses Forschungsvorhaben. Hierzu wurde durch die Unterbeauftragung des DIN e. V. unter anderem auch der Kontakt zum DIN-Normungsausschuss Informationstechnik und Anwendung (NIA) genutzt.

Existierende Standards & Normen (Auszug)	
DIN SPEC 16597	Terminologie für Blockchains
EIN EN ISO 22739	Blockchain und Technologie für verteilte elektronische Journale – Begriffe
ISO 23257	Blockchain und Technologie für verteilte elektronische Journale – Referenzarchitektur
Laufende Aktivitäten im Bezug auf Standardisierung und Normierung (Auszug)	
DIN CEN/CLC/TS XXXJT19002	Projekt: Dezentrales Identitätsmanagementmodell auf der Grundlage von Blockchain und anderen Distributed-Ledger-Technologien - Teil 1: Generischer Referenzrahmen
ISO/AWI TR 19626-3	Projekt: Processes, data elements and documents in commerce, industry and administration -Trusted communication platforms for electronic documents - Part 3: Blockchain-based implementation guideline
ISO/AWI TS 23516	Blockchain and Distributed Ledger Technology - Interoperability Framework
ISO/DTR 16340	Projekt: Application of blockchain-based traceability platform for cold chain food
ISO/DTR 23644	Projekt: Blockchain and distributed ledger technologies (DLTs) - Overview of trust anchors for DLT-based identity management
ISO/PRF TR 6039	Projekt: Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems
ISO/TR 24374	Projekt: Financial services - Security information for PKI in blockchain and DLT implementations
ISO/WD 5909	Projekt: Datenaustauschprozesse von auf Blockchain basierenden bezieharen Seefrachtbriefen im Zusammenhang mit E-Commerce-Plattformen
ISO/WD TR 6277	Projekt: Blockchain and distributed ledger technologies - Data flow model for blockchain and DLT use cases
ISO/WD TR 23642	Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues

Tabelle 2: Auszug über existierende Normen, Standards und laufende Aktivitäten

Aufbauend auf den Recherchen wurde anschließend die DIN SPEC entwickelt. Die nachfolgende Tabelle beschreibt den entsprechenden Entwicklungsprozess.

Schritt	Tätigkeiten
1) Initiierung	<ul style="list-style-type: none"> Anfrage durch Initiator*in an DIN Interne Prüfung: Abstimmung mit den relevanten Normenausschüssen (NA) Freigabe zur Fortführung des Initiierungsprozesses durch den Vorsitzenden des Vorstands von DIN In Abstimmung mit Initiator*in Erstellung eines Geschäftsplans Veröffentlichung des Geschäftsplans auf der DIN-Webseite für 4 Wochen zur Kommentierung durch die Öffentlichkeit sowie Anmeldung zum Kick-off Prüfung der Kommentare zum Geschäftsplan und Entscheidung bzgl. der Genehmigung der Anfrage durch die Geschäftsleitung von DIN
2) Erarbeitung	<ul style="list-style-type: none"> Kick-off Treffen: Konstituierung des Konsortiums durch Annahme des Geschäftsplans, Wahl der Konsortialleitung, Detailplanung des Projekts Schließen des Vertrags zwischen Initiator*in und DIN Erarbeitung des Manuskripts durch das Konsortium Entwurfsveröffentlichung für 2 Monate (optional) Verabschiedung des Entwurfs durch das Konsortium (Mehrheitsbeschluss) Konsortium entscheidet über Einarbeitung der Kommentare
3) Veröffentlichung	<ul style="list-style-type: none"> Verabschiedung der DIN SPEC durch das Konsortium Mehrheitsbeschluss Genehmigung durch die DIN-Geschäftsleitung Eintragung in die Normendatenbanken Bekanntmachung in DIN-Mitteilungen und im Webauftritt von DIN Veröffentlichung der kostenfreien DIN SPEC als PDF-Datei über den Beuth WebShop
4) Überprüfung	<ul style="list-style-type: none"> Maximale Lebensdauer einer DIN SPEC von 6 Jahren je Ausgabe. Die erste Überprüfung erfolgt 3 Jahre nach Veröffentlichung durch DIN in Abstimmung mit dem DIN-SPEC-Konsortium: Beibehaltung Zurückziehung Neuausgabe DIN SPEC (Revision) Antrag auf Überführung in eine Norm

Tabelle 3: Entwicklungsprozess der DIN SPEC

Gemäß dem beschriebenen Prozess (Schritt 1-3) wurden in Zusammenarbeit mit dem DIN e. V. und im Rahmen der DIN-SPEC-Erstellung die in AP 2 (siehe Kap. 2.2) herausgearbeiteten Anforderungen und Merkmale einer Blockchain im Supply-Chain-Management weiter ausgeführt und mit Fallbeispielen ergänzt.

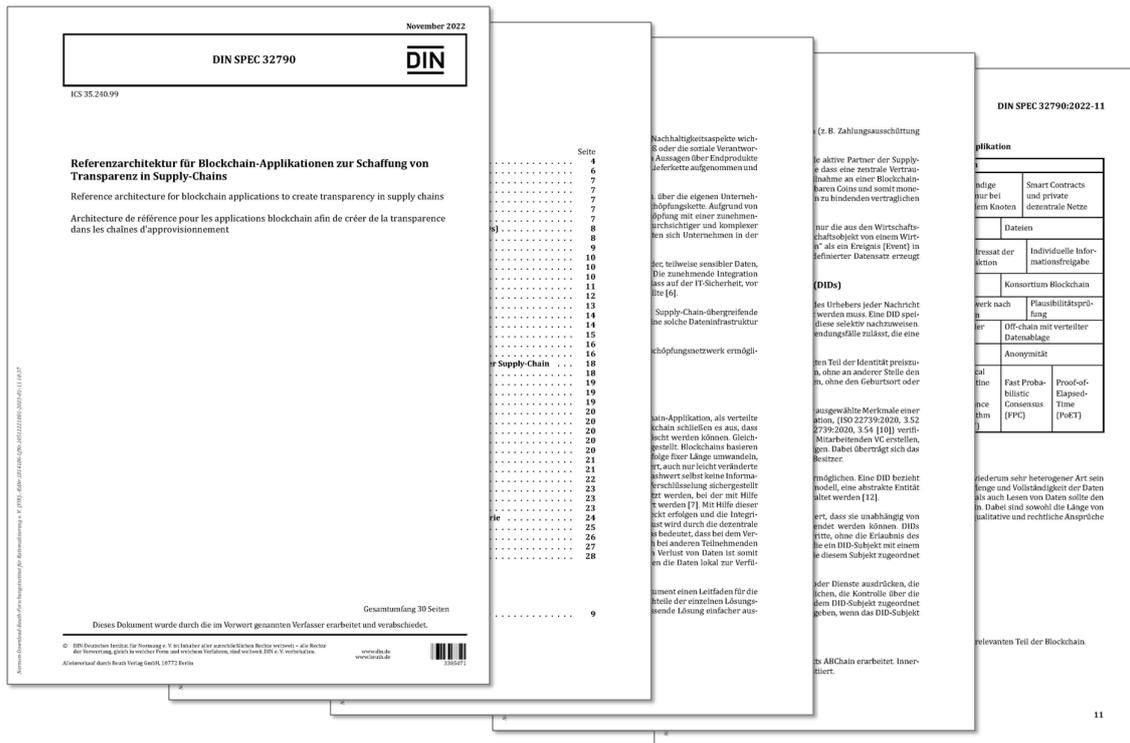


Abbildung 10: Auszug aus der DIN SPEC 32790

Im Rahmen der Erarbeitung der DIN SPEC 32790 (Referenzarchitektur für Blockchain-Applikationen zur Schaffung von Transparenz in Supply-Chains) wurde die entwickelte Morphologie anhand verschiedener Szenarien und konkreten Fallbeispielen betrachtet. Auf Basis dessen wurde die in AP 2 entwickelte Morphologie leicht angepasst. Die angepasste Morphologie ist in der folgenden Abbildung dargestellt.

Merkmal	Ausprägung			
Grad der Datenverteilung	Vollständige Daten je Knoten	Knoten mit und ohne vollständige Daten	Vollständige Daten nur bei zentralem Knoten	Smart Contracts / Private dezentrale Netze
Abzuspeichernde Daten	Hash-Werte		Code	Dateien
Informationsfreigabe	Keine Begrenzung	Für Adressat der Transaktion und alle Folgenden	Für Adressat der Transaktion	Individuell
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
Konsensalgorithmus	Proof of Work (PoW)	Proof of Stake (PoS)	Practical Byzantine Fault Tolerance Algorithm (PBFT)	...

Abbildung 11: Angepasste Morphologie der Blockchain-Technologie für die DIN SPEC 32790

Wie zuvor erwähnt, wurden bei der Erarbeitung der DIN SPECs verschiedene Fallbeispiele betrachtet. Im Folgenden sind beispielhaft drei dieser Fallbeispiele dargestellt.

Fallbeispiel a: CO₂-Fußabdruck

Motivation: Da 80 Prozent des CO₂-Fußabdrucks eines Produkts aus der Lieferkette stammen, ergeben sich immense Einsparpotenziale durch einheitliche und verifizierte Weitergabe der Werte. Dies ist heutzutage mit sehr hohem Aufwand verbunden, da nur auf veraltete 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.

Ziele und Vorgehen: Um ein Maximum an Vertrauen für die Primärdaten der Lieferketten-Akteure 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 CO₂-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*).

Innovationen und Perspektiven: Durch die Nutzung von Blockchain-Applikationen ergibt sich die Möglichkeit, verifizierte Werte über verschiedene Branchen hinweg auszutauschen und dadurch einen hohen Grad an Vertrauen zu gewinnen, ohne sensible Daten offenzulegen. Der Aufwand für die Berechnung des CO₂-Fußabdrucks der Lieferkette wird durch automatisierte Verifizierung und Berechnung erheblich reduziert, da Kosten für die Verifizierung von Transaktionen eingespart werden können.

Fallbeispiel b: Rückverfolgung von Lebensmitteln

Motivation: Aktuelle Studien zeigen, dass für über 80 Prozent der Bevölkerung das Thema Ernährung eine wichtige Rolle spielt. Dabei ist die Sicherheit der Lebensmittel bezüglich ausreichender Qualität die wichtigste Forderung. Gleichzeitig besteht ein vergleichsweise geringes Vertrauen in die Lebensmittelwirtschaft, diese zu gewährleisten. 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.

Ziele und Vorgehen: Im Vorhaben werden 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 gewährleisten und bedarf keiner zentralen „dritten“ Instanz, beispielsweise eines Plattformanbieters. Im Vorhaben wird untersucht, welche Daten im System erfasst werden müssen und wie das System im Sinne der Unternehmen wirtschaftlich auszulegen ist. Die IT-Lösung wird anhand zweier konkreter Anwendungsfälle im Testbetrieb bei Anwender:innen erprobt.

Innovationen und Perspektiven: Die IT-Lösung soll 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 Konsument:innen einzuleiten. Dies unterstützt die Effektivität von Maßnahmen, wie z. B. gezieltere Rückrufaktionen, wirkt damit einer Verknappung von Lebensmitteln entgegen und stärkt das Vertrauen der Bevölkerung in die Lebensmittelwirtschaft.

Fallbeispiel c: Conflict-Mineral

Motivation: Seit Anfang 2020 gilt die sogenannte Conflict-Minerals-Regulation der Europäischen Union für die Sorgfaltspflicht bestimmter Ressourcen in der Lieferkette. 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 ist und ausbeuterischen Arbeitsbedingungen ausgesetzt ist. Daher ergibt sich eine große Verantwortung für Unternehmen entlang der Wertschöpfungskette, dafür Sorge zu tragen, dass ihre Lieferketten von solchen Konflikten befreit ist.

Ziele und Vorgehen: Durch die Erstellung eines digitalen Zwillings der Rohmaterialien können diese digital entlang der Lieferkette rückverfolgt werden. Jeder Teilnehmer eines Blockchain-Netzwerks kann 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.

Innovationen und Perspektiven: 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.

Das Ziel von AP 4, die Beauftragung einer DIN SPEC, um die Normung erarbeiteter Formate anzustoßen, wurde im Projekt erfolgreich erarbeitet. Die entstandene DIN SPEC stellt die Überführung der Projektergebnisse in eine Normung des DIN-Standards dar.

2.5 AP 5: Gestaltungsleitfaden zur Integration einer Blockchain-Applikation

Arbeitspaket 5 hat zum Ziel, den Gestaltungsleitfaden vorzustellen, anhand dessen die Anforderungen der anwendenden Unternehmen an Blockchain-Applikationen herausgearbeitet werden können. Der Leitfaden soll, durch die Abfrage und anschließende Identifizierung der unterschiedlichen Merkmale einer Blockchain-Applikation, der Implementierung im entsprechenden Unternehmen dienen.

2.5.1 Aufbau des Gestaltungsleitfadens

Mithilfe des Gestaltungsleitfadens sollen die unterschiedlichen Merkmale einer Blockchain-Applikation abgefragt werden, die durch die Usecases/Anforderungen der anwendenden Unternehmen beeinflusst werden. Die Fragen sollen so gestellt werden, dass sie auch von Personen beantwortet werden können, die kein tiefgreifendes Wissen über die Blockchain-Technologie haben. Es wird jedoch davon ausgegangen, dass die entsprechende Person zumindest die Grundlagen, die sowohl der DIN SPEC als auch diesem Abschlussbericht zugrunde liegen, gelesen hat. Der Fragebogen ist generell so aufgebaut, dass die Fragen im Freitext beantwortet werden können. Die Ausprägungen werden anschließend über Textbausteine und Schlagwörter zugeordnet, die in den Antworten enthalten sind. Dies soll die Zugänglichkeit des Fragebogens erhöhen.

Das maßgeblichste Gestaltungsmerkmal einer Blockchain ist die Art der Blockchain, was sich auch hinter den Merkmalsausprägungen des Lese- und Schreibzugriffs verbirgt. Die entsprechenden Ausprägungen können sein: öffentliche Blockchain, private Blockchain oder konsortiale Blockchain. Aus diesem Grund wird zunächst die Frage gestellt, wem Zugriff gewährt wird.

Fragestellung	Erläuterung
Wer soll auf die Blockchain zugreifen dürfen? (Das bedeutet noch nicht, dass alle alles lesen dürfen.)	Mit dieser Frage soll ermittelt werden, ob die Blockchain-Applikation prinzipiell zugänglich für die breite Öffentlichkeit sein soll (öffentliche Blockchain) oder ob der Zugang beschränkt werden soll. Hierbei muss noch zwischen einer Freigabe neuer Teilnehmender durch eine berechnigte Gruppe oder eine einzelne Instanz unterschieden werden. Hat nur eine einzelne Instanz das Recht, neue Teilnehmende zur Blockchain-Applikation zuzulassen, spricht man von einer privaten Blockchain. Wird der Zugriff durch eine Gruppe an rechtlichen Personen – also ein Konsortium – geregelt, spricht man von einer konsortialen Blockchain.
Sind alle Parteien gleichberechtigt?	Die nächste Frage zielt noch mal auf das gleiche Merkmal ab und verifiziert die vorherige Aussage.

Fragestellung	Erläuterung
Dürfen alle Parteien auf alle Daten zugreifen oder wie sollen Zugriffsrechte verteilt werden?	Gibt es bei dieser Frage viele unterschiedliche Freigabevarianten, deutet dies direkt auf eine individuelle Informationsfreigabe hin. Kann die Freigabe direkt auf den Adressaten beschränkt werden, so können auch die entsprechenden Ausprägungen gewählt werden.
Welche Daten tauschen Sie mit den Partnern entlang Ihrer Lieferkette aus? (Dokumente/Dateien, Informationen in Textform) Um welches Volumen/Menge handelt es sich?	Hierüber soll zum einen abgeschätzt werden, welche Arten von Daten generell zugelassen werden sollen und zum anderen, wo diese gespeichert werden können. Sollen viele Dokumente und Dateien ausgetauscht werden, so bietet sich in der Regel eine Kombination aus Off- und On-Chain-Datenspeicherung an. Bei einer dezentralen Datenablage, wie es bei einer Blockchain der Regelfall ist, sollten keine großen Datenvolumen ausgetauscht werden, weil ansonsten die benötigten Serverkapazitäten und Energiemengen für den Datenaustausch sehr groß werden.
Sollen alle Partner (mit oder ohne Zugriffsbeschränkung) die Daten bei sich speichern, um ggf. direkt und jederzeit Zugriff darauf haben zu können?	Diese Frage schließt an der vorherigen an und soll nochmal auf die verteilte oder zentrale Datenablage eingehen. Hierbei gibt es nicht nur die Möglichkeiten, die Blockchain an sich dezentral oder zentral zu speichern, sondern auch ggf. verknüpfte Dokumente, die offchain gespeichert sind zentral und dezentral abzulegen.
Wie wichtig ist Ihnen der Schutz vor Datenverlust durch bspw. defekte Server?	Aufschluss über diese Fragestellung geben die jeweiligen Konsensmechanismen, mit denen ein Konsens darüber gefunden wird, wie neue Blöcke gebildet werden und an bisherige Blöcke angehängt werden können. Das Regelwerk zur Datenaufnahme stellt in Bezug auf diese Fragestellung einen weiteren relevanten Faktor dar, da die entsprechenden Ausprägungen aufzeigen, auf welche Charakteristika bei der Datenaufnahme besonders Wert gelegt wird.
Sollen nur bestimmte Daten/Informationen in die Blockchain oder kann das jeder Partner frei entscheiden?	Aufschluss über diese Fragestellung geben die jeweiligen Konsensmechanismen, mit denen ein Konsens darüber erstellt wird, wie neue Blöcke gebildet werden und an bisherige Blöcke angehängt werden können. Das Regelwerk zur Datenaufnahme stellt in Bezug auf diese Fragestellung einen weiteren relevanten Faktor dar, da die entsprechenden Ausprägungen aufzeigen, auf welche Charakteristika bei der Datenaufnahme besonders wert gelegt wird.
Sollen bzw. dürfen alle Partner, die am Datenaustausch beteiligt sind, für alle anderen Teilnehmenden an der Blockchain-Applikation bekannt sein?	Diese Frage gibt Auskunft über die jeweilige Ausprägung bzw. Variante der Bekanntheit der Teilnehmenden in der Blockchain-Applikation. Neben der vollkommenen Bekanntheit aller am Datenaustausch beteiligten Teilnehmern liegt die Möglichkeit der vollkommenen Anonymität aller anderen Teilnehmenden an der Blockchain-Applikation vor. Die Variation der Pseudonymität bildet ein Mittelmaß, in dem der öffentliche Schlüssel zum einen grundsätzlich geschützt ist, aber zum anderen die Möglichkeit zur Profilerstellung anhand einer festen Adresse im Netzwerk besteht.

Tabelle 4: Fragebogen des Gestaltungsleitfadens

2.5.2 Auswertung und Gestaltung der Blockchain-Applikation

Die durchgeführten Interviews wurden primär genutzt, um einen Rückschluss auf die zu applizierende, unternehmensspezifische Art der Blockchain zu ziehen. Inbegriffen ist die Priorisierung bzw. Ausgestaltung der Ausprägungen der jeweiligen Blockchain Kategorien.

Voranehend erfolgt das Ausfüllen der Umfrage, welches analog zu den Interviews aufgebaut ist und, aus Freitextfeldern bestehend, individuelle Antworten ermöglicht.

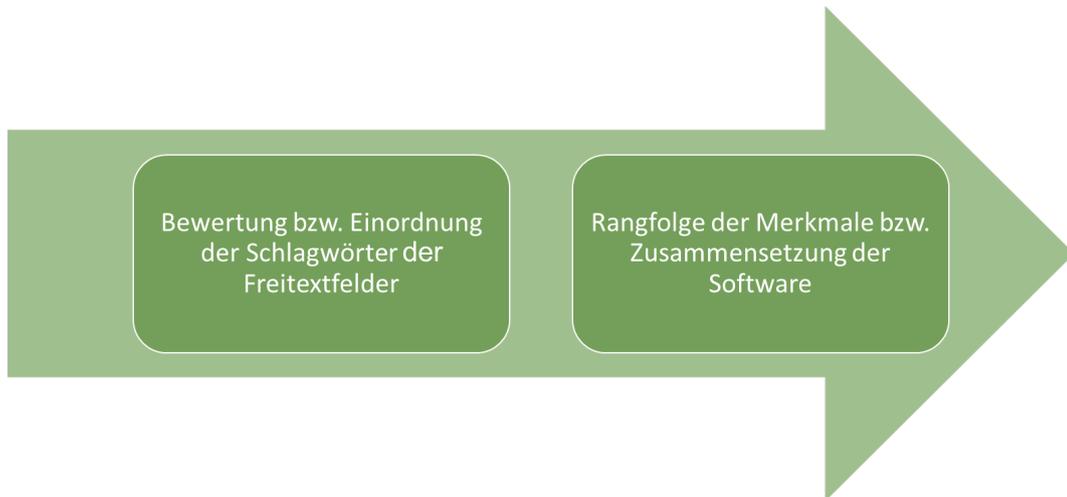


Abbildung 12: Vorgehen zur Auswertung

Im Anschluss wird jede Antwort auf Schlagwörter untersucht, welche in der nachfolgenden Tabelle (s. nächste Seite) nach Merkmal und Frage sortiert aufgelistet sind. Diese Tabelle ist so ausgelegt, dass die Spalten die drei existenten Ausprägungen einer Blockchain behandeln und jede vorliegende Zelle merkmals- und Blockchain-spezifische Inhalte wiedergibt. Die resultierende Blockchain-Kategorie mit den meisten im Validierungsgespräch wiederzufindenden Schlagwörtern steht zur Implementierung im entsprechenden Unternehmen zur Verfügung.

Das Ziel von AP 5, die Umsetzung eines Entwurfs von Gestaltungsempfehlungen zur Integration einer Blockchain-Applikation, wurde erfolgreich im Projekt erreicht. Der dabei entstandene Gestaltungsleitfaden zur Integration einer Blockchain-Applikation dient der Abfrage und anschließenden Identifizierung der unterschiedlichen Merkmale einer Blockchain-Applikation, die durch die Usecases/Anforderungen der anwendenden Unternehmen beeinflusst werden.

Merkmale	Frage	Private Blockchain	Konsortial-Blockchain	Öffentliche Blockchain
Lese- und Schreibzugang	5	<ul style="list-style-type: none"> ▪ Installierbarkeit, Bedienbarkeit; Automatisierte Übertragung der Daten; einfache Systemvoraussetzungen 	<ul style="list-style-type: none"> ▪ Installierbarkeit, Bedienbarkeit; automatisierte Übertragung der Daten; einfache Systemvoraussetzungen für KMU 	<ul style="list-style-type: none"> ▪ Installierbarkeit, Bedienbarkeit, Umgang mit heterogenen IT-Systemen, Automatisierte Übertragung der Daten
	7	<ul style="list-style-type: none"> ▪ genehmigungspflichtig, kontrolliert durch eine Autorität (zentrale Verwaltungsinstanz), Zugang mittels individueller Leserechte 	<ul style="list-style-type: none"> ▪ Umgang mit heterogenen IT-Systemen ▪ Gemischt (Definierte Teilnehmende); Konsortium aus mehreren Teilnehmenden trifft Entscheidung über Verteilung der Lese- und Schreibrechte 	<ul style="list-style-type: none"> ▪ Jeder; genehmigungsfrei; keine zentrale Autorität
Abzuspeichernde Daten	4	<ul style="list-style-type: none"> ▪ Kapazitäten bzgl. Datengrößen 	<ul style="list-style-type: none"> ▪ eingeschränkte Flexibilität 	<ul style="list-style-type: none"> ▪ Datenschutz bzw. Transparenz
	6	<ul style="list-style-type: none"> ▪ Speicherung von sensiblen Daten durch Vergabe von Leserechten möglich 	<ul style="list-style-type: none"> ▪ Speicherung von sensiblen Daten durch Vergabe von Leserechten möglich 	<ul style="list-style-type: none"> ▪ keine kritischen Daten aufgrund von Transparenz
	8	<ul style="list-style-type: none"> ▪ Hashwerte, sehr geringe Datengröße; mehr Transaktionen mit höheren Geschwindigkeiten (kostengünstiger) 	<ul style="list-style-type: none"> ▪ Code, mittlere Größe; höhere Prozess- und Interaktionsgeschwindigkeit 	<ul style="list-style-type: none"> ▪ Dateien, sehr große Datenmengen (hohe Transaktionskosten und -geschwindigkeiten aufgrund Vielzahl an Nodes)
Verteilte Datenablage	9	<ul style="list-style-type: none"> ▪ Ausschließlich On-Chain (Steuerung u. Verwaltung durch zentrale Instanz); Dateien somit nicht möglich 	<ul style="list-style-type: none"> ▪ Off-Chain mit zentraler Datenablage, geringe Datenmenge auf Blockchain, bessere Skalierbarkeit, hohe Verfügbarkeit und Sicherheit vor Datenverlust; hoher Zentralisierungsgrad 	<ul style="list-style-type: none"> ▪ Off-Chain mit verteilter Datenablage, geringe Datenmenge auf Blockchain, bessere Skalierbarkeit; Datenablage hat Hochverfügbarkeit eines verteilten Systems
Regelwerk zur Daten-aufnahme	10	<ul style="list-style-type: none"> ▪ Plausibilitätsprüfung und Validierung von Transaktionen durch zentrale Instanz, Regelwerk nach Knoten 	<ul style="list-style-type: none"> ▪ Prüfung nach Datenstruktur und Plausibilitätsprüfung (Transaktion muss durch bestimmte Mehrheit der Blockchain-Teilnehmenden angenommen werden; Konsenserzielung); Regelwerk nach Knoten 	<ul style="list-style-type: none"> ▪ keine Prüfung der Daten (alles wird angenommen)
Bekanntheit der Teilnehmenden	11	<ul style="list-style-type: none"> ▪ Jeder Teilnehmende ist bekannt 	<ul style="list-style-type: none"> ▪ Pseudonymität, öffentlicher Schlüssel ist grundsätzlich geschützt 	<ul style="list-style-type: none"> ▪ komplette Anonymität des Senders und Empfängers
Informations-freigabe	12	<ul style="list-style-type: none"> ▪ Einsicht spezifischer Informationen bzw. Schreibrechte; individuelle Informationsfreigabe 	<ul style="list-style-type: none"> ▪ Zugriffsrechte verteilen, spezifisch freigegebene Informationen 	<ul style="list-style-type: none"> ▪ Einsicht aller veröffentlichten Daten; keine Begrenzung zur Erreichung max. Transparenz

Tabelle 5: Merkmale bzgl. Auswertung

2.6 AP 6: Validierung der Ergebnisse

Arbeitspaket 6 hat zum Ziel, die zuvor erbrachten Ergebnisse zu validieren. Dabei soll die Anwendung des Gestaltungsleitfadens von Fallstudien der Validierung dienen. Darauf aufbauend soll der zukünftige Forschungsbedarf abgeklärt werden.

Die Validierung der vorgestellten Blockchain-Applikation erfolgte durch Interviews. Die Validierungsgespräche haben bestimmte Ziele im Fokus und wurden zunächst durch einen angefertigten Validierungsgesprächsleitfaden strukturiert (s. STEFFEN U. DOPPLER 2019, S. 31) . Bedient wurde sich der offenen bzw. allgemeinen Fragestellung, sodass umfangreiche und individuelle Antworten ermöglicht werden (s. STEFFEN U. DOPPLER 2019, S. 31). Vertiefend handelt es sich um eine teilstrukturierte qualitative Befragung, die zum einen leitfadenbasiert vorliegt und zum anderen individuelle bzw. freie Antwortmöglichkeiten zulässt (s. STEFFEN U. DOPPLER 2019, S. 39). Um die Ergebnisse des Validierungsgesprächs anschließend auch, beispielsweise für ein Forschungsprojekt, nutzen zu können, wird eine zuvor erstellte Einverständniserklärung hinzugezogen (s. STEFFEN U. DOPPLER 2019, S. 32).

Im Anschluss an die einleitenden Daten bzw. Faktenfragen zu der befragten Person werden die Verständlichkeit und Nachvollziehbarkeit des behandelten Themas herausgearbeitet. Dies trägt maßgeblich zum Verständnis des entsprechenden Anwendungsfalls bei und dazu, Verbesserungspotenziale aufzudecken. Insgesamt wurden zwei Interviews durchgeführt, die auf einem zuvor entwickelten Gestaltungsleitfaden basieren. Befragt wurden dazu ein operativer Projektleiter eines anwendungsnahen Forschungsprojekts und eine Führungskraft eines etablierten Herstellungsunternehmens.

Um ein Tool zu entwickeln, das diesen Prozess digitalisiert bzw. automatisiert, wurde eine Online-Umfrage erstellt, welche umfangreiche individuelle Antwortmöglichkeiten zulässt. Anhand eines Auswertungsleitfadens ist es möglich, eigenständig auf eine passende Blockchain-Kategorie zu schließen. Diese Vorgehensweise fördert das Grundverständnis für die einzelnen Merkmale der Blockchain-Arten und ihre Wechselwirkungen.

2.6.1 Fallstudie 1: Projekt SiLKe

Dieser Abschnitt dient der Darlegung der Durchführung sowie der wesentlichen Ergebnisse der beiden durchgeführten Interviews. Die nachfolgende Tabelle bildet exemplarische die genaue Durchführung des Validierungsgesprächs ab.

I) Einleitende Daten zum Unternehmen und der Person	
In welcher Branche sind Sie tätig?	Aktuell bin ich tätig am FIR e. V. und arbeite speziell am Forschungsprojekt SiLKE. Dieses Projekt entspringt der Branche der Lebensmittelindustrie.
Welche Rolle spielen Sie für das Unternehmen bzw. welche Position nehmen Sie ein?	Positioniert bin ich als Operativer Projektleiter des Forschungsprojekts SiLKE.
II) Beschreibung des Anwendungsfalls und der Anforderungen	
Beschreiben Sie den Kontext, aus dem das Projekt entstanden ist.	Das Projekt bezieht sich auf die Lebensmittellieferkette vom Ursprung der Erzeugung (Fischerei, Bauern etc.) bis zum Lebensmitteleinzelhandel, um die Lebensmittelsicherheit zu erhöhen.
Welche Anforderungen richten sich dabei an die Blockchain-Applikation?	Die Rückverfolgbarkeit der Lebensmittel muss im Anschluss an die Blockchain-Applikation optimiert bzw. erhöht sein. Außerdem soll dies bei bestmöglicher Fälschungssicherheit und hoher Datensouveränität erfolgen. Die Erleichterung von Rückrufen sowie die Speicherung von Dateien wie Zertifikaten spielen zudem eine wichtige Rolle.
Was stellt sich als Ihre größten Herausforderungen hinsichtlich des Austauschs von Daten mit Partnern in Ihrer Lieferkette heraus?	Als größte Herausforderung sehe ich zunächst die Bereitschaft, an der Blockchain teilzunehmen und Initialaufwand zu betreiben sowie nachfolgend die Bereitschaft, Daten zu teilen, aufgrund des Datenschutzes.
Welche Anforderungen ergeben sich hinsichtlich des Zugangs zur Blockchain?	Einführend stellen bereits die Installierbarkeit sowie die nutzerfreundliche Bedienbarkeit eine Anforderung an die Teilnehmenden der Blockchain. Anschließend bildet die automatisierte Übertragung der Daten auf die entsprechenden Nodes der Blockchain eine Herausforderung. Ebenfalls ist es eine Herausforderung für die Teilnehmenden deutlich bei Betrachtung der einfachen Systemvoraussetzungen die Kleinstunternehmen zu erkennen, insbesondere Landwirtschaftliche Betriebe, die bisher kaum Kontakt zu IT-Systemen haben. Als erweiterte Betrachtung ist der Umgang mit heterogenen IT-Systemen entlang der Lieferkette von Bedeutung, da diese unterschiedliche Kenntnisse für die Nutzung voraussetzen.
Gibt es sensible Daten, die Sie entlang der Lieferkette austauschen möchten, die besonders behandelt werden müssen?	Besonders die Kunden-Lieferantenbeziehungen dürfen nicht aufgedeckt werden und müssen sensibel behandelt werden. Die ausgetauschten bzw. gespeicherten Daten sollen individuell mit Leserechten freigegeben werden und nur für diese zugänglich sein.

III) Beantwortung des Fragebogens bzw. Durchgehen des Gestaltungsleitfadens:	
Wer soll auf die Blockchain zugreifen dürfen?	Nachgelagert sollen auch die Konsument:innen im Supermarkt die Lieferkette nachverfolgen können; hier sollen allerdings nur stark eingeschränkte Daten zur Verfügung stehen (bisher nicht im Fokus). Nicht jeder soll aber an der Blockchain teilhaben können, nur bestimmte, definierte Teilnehmende. Manche Daten sollen nicht auf der Blockchain gespeichert werden, da diese sehr sensibel sind.
Welche Größe an Daten tauschen Sie mit entsprechenden Partnern entlang Ihrer Lieferkette aus?	Es sollen auch Zertifikate und Dateien abgespeichert werden können.
Stellt die dezentrale Datenablage für Sie einen Mehrwert dar bzw. sehen Sie in diesem Kontext eine Chance oder ein Risiko?	Ja, die dezentrale Datenablage ist generell für die Blockchain selbst wichtig. Für bestimmte Dateien, wie besonders die kritischen Dateien, ist es wichtig, dass diese nicht dezentral gespeichert werden, um das Risiko eines Datenleaks zu minimieren. Der Grad der Datenverteilung soll sich so gestalten, dass vollständige Daten je Knoten vorliegen.
Wie sollen die Daten vor der Aufnahme geprüft werden?	Die Daten müssen für alle Partner in der Lieferkette in der Struktur von EPCIS-Events vorliegen und müssen, als Grundlage für einen effizienten Informationsaustausch, dem GS1-Standard entsprechen.
Spielt die Bekanntheit der an dem Softwareaustausch teilnehmenden Personen eine wichtige Rolle?	Gerade die Kunden-Lieferantenbeziehungen dürfen nicht aufgedeckt werden. Dennoch sind aber eine teilweise vorliegende Bekanntheit sowie Anonymität der Teilnehmenden, abgrenzend von Kunden-Lieferantenbeziehungen, möglich.
Wer soll die Daten einsehen können?	Bei dieser Fragestellung ist es von erheblicher Relevanz, zwischen den einzelnen Rollen bzw. Arten der Blockchain-Nutzer zu differenzieren: <ul style="list-style-type: none"> • Bei Betrachtung der Rolle der Endkonsumentin/des Endkonsumenten darf jeder veröffentlichte Daten einsehen. • Im Hinblick auf die Rolle der Behörde sind nur die spezifisch freigegebenen Daten für den Zugriff inbegriffen. • Genauso ist bei Heranziehen der Rolle der Teilnehmenden zu beachten, dass nur spezifische Informationen gelesen werden dürfen und für manche Dinge Schreibrechte bestehen. <p>➔ Individuelle Informationsfreigabe</p>
IV) Überprüfung der Ergebnisse aus dem Gestaltungsleitfaden und der Vergleich mit den entsprechenden Anforderungen	
Passt das zu den Anforderungen?	Ja, die durch die Validierung resultierenden Ergebnisse passen generell zu den Anforderungen an die Blockchain-Applikation.
Liefert der Gestaltungsleitfaden einen Mehrwert oder hätten Sie auch ohne die Morphologie ausfüllen können?	Ja, der Gestaltungsleitfaden ist definitiv hilfreich und trägt zum weiteren Verständnis bei, da nicht alle Ausprägungen selbsterklärend sind.

Tabelle 6: Darstellung des durchgeführten Validierungsgespräch

Auf Basis der Ergebnisse des Interviewpartners ergibt sich folgende Ausprägung in der ausgearbeiteten Morphologie:

Merkmals	Ausprägung			
Grad der Datenverteilung	Vollständige Daten je Knoten	Knoten mit und ohne vollständige Daten	Vollständige Daten nur bei zentralem Knoten	Smart Contracts / Private dezentrale Netze
Abzuspeichernde Daten	Hash-Werte		Code	Dateien
Informationsfreigabe	Keine Begrenzung	Für Adressat der Transaktion und alle Folgenden	Für Adressat der Transaktion	Individuell
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
Konsensalgorithmus	Proof of Work (PoW)	Proof of Stake (PoS)	Practical Byzantine Fault Tolerance Algorithm (PBFT)	...

Abbildung 13: Angepasste Morphologie für die Fallstudie Projekt Silke

Der befragte Interviewpartner ist davon überzeugt, dass der Gestaltungsleitfaden ein wichtiges Instrument zum grundlegenden Verständnis darstellt und weiterhin genutzt werden sollte. Außerdem zeigt der Anwendungsfall auf, dass die unternehmensspezifischen Anforderungen an die Blockchain mit den Ergebnissen der Validierung übereinstimmen. Dies lässt sich anhand der abschließenden Fragestellung nachweisen. Damit einhergehend wurden somit die Relevanz der Blockchain-Applikation für die Praxis sowie eine wesentliche Applikabilität in der Praxis bestätigt.

Dennoch lässt sich das Resultat des Validierungsgesprächs mit dem Interviewpartner nicht verallgemeinern und auf andere Branchen übertragen, da deutlich die Relevanz für die Lebensmittelindustrie hervorgehoben wurde.

Bezogen auf die Anwendbarkeit der Blockchain schenkte der Interviewpartner maßgeblich der Anforderung an den grundlegenden Zugang zur Blockchain Beachtung, da er in diesem Punkt die umfangreichste Herausforderung für die Teilnehmenden sieht. Hierbei betont der Befragte die Schwierigkeit für Kleinstunternehmen, erstmals die entsprechenden Systemvoraussetzungen zu erfüllen. Weiterhin wurden in Bezug auf die Applikation der Blockchain weitere befürchtete Herausforderungen benannt, wie die Bereitschaft, Daten entlang der Lieferkette zu teilen. Aus den aufgezeigten Herausforderungen folgernd ist zu erkennen, dass es sich hierbei maßgeblich um initiale Schritte des Blockchain-Gebrauchs handelt.

Von besonderer Relevanz für die Auswertung der Validierung ist die Differenzierung der Teilnehmenden der Blockchain, die zugangsberechtigt sein sollen. Die durch den Interviewpartner beschriebenen, berechtigten Teilnehmenden schließen bereits die Applikation einer öffentlichen Blockchain aus, da es sich um zuvor definierte Teilnehmende handelt. Außerdem wirkt der im

Validierungsgespräch beschriebene Austausch sensibler Daten einer öffentlichen Blockchain entgegen. Eine direkte Auswahl zwischen einer privaten und einer Konsortial-Blockchain kann dennoch nicht vorgenommen werden, da beispielsweise die in einer privaten Blockchain genutzten On-Chain-Datenablage eine Speicherung der gewünschten Dateien ausschließt (siehe angehängter Gestaltungsleitfaden). Die genauere Differenzierung der unternehmensspezifischen Blockchain-Art lässt sich somit erst nach detaillierterer Nutzung des angefügten Leitfadens zur Selbstausswertung bestimmen.

2.6.2 Fallstudie 2: Anonymes Herstellungsunternehmen

Zusätzlich wurden der Gestaltungsleitfaden wie auch die angepasste Morphologie anhand einer zweiten Fallstudie validiert. Da es sich hierbei jedoch um ein anonymes Herstellungsunternehmen handelt, seien im Folgenden nur die angepasste Morphologie wie auch die Bewertung des Gestaltungsleitfadens dargestellt.

Merkmale	Ausprägung			
Grad der Datenverteilung	Vollständige Daten je Knoten	Knoten mit und ohne vollständige Daten	Vollständige Daten nur bei zentralem Knoten	Smart Contracts / Private dezentrale Netze
Abzuspeichernde Daten	Hash-Werte		Code	Dateien
Informationsfreigabe	Keine Begrenzung	Für Adressat der Transaktion und alle Folgenden	Für Adressat der Transaktion	Individuell
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
Konsensalgorithmus	Proof of Work (PoW)	Proof of Stake (PoS)	Practical Byzantine Fault Tolerance Algorithm (PBFT)	...

Abbildung 14: Angepasste Morphologie für die Fallstudie Projekt Anonymes Herstellungsunternehmen

Der befragte Interviewpartner hebt die Bedeutung des Gestaltungsleitfadens als elementares Werkzeug für das Verständnis hervor. Grundsätzlich fand er die Beantwortung der Fragen verhältnismäßig schwer, da sie als abstrakt wahrgenommen wurden. Dies würde insbesondere bei interviewten Personen, welche sich mit Blockchain-Technologien noch nicht im Detail auseinandergesetzt haben, am Anfang eine Hemmschwelle darstellen. Weiterhin merkte der Interviewpartner an, dass die Wichtigkeit der benötigten Daten deutlicher herausgestellt werden könnte. Nichtsdestotrotz wurden die Anwendbarkeit und die Auswertbarkeit anhand der Morphologie als gut empfunden.

Das Ziel von AP 6, die Durchführung der Validierung der zuvor erbrachten Ergebnisse, wurde erfolgreich im Projekt erarbeitet. Die dabei entstandenen konkreten Fallstudien dienen zur Validierung der Ergebnisse.

3 Wissenschaftlich-technischer und wirtschaftlicher Nutzen für KMU

Im Kontext der Digitalisierung stehen KMU des produzierenden Gewerbes vor vielfältigen Herausforderungen im Hinblick auf Produkte und Lieferketten sowie Datensicherheit und Datenschutz. Produkte werden zunehmend komplexer und sind gekennzeichnet von einer steigenden Individualisierung bei immer kürzeren Produktlebenszyklen und einer stetig wachsenden Anzahl von Partnern in der Wertschöpfungskette. Zugleich entstehen in den Lieferketten hochkomplexe Lieferantenbeziehungen in dynamischen Wertschöpfungsnetzwerken, während Datensicherheit und Datenschutz im Rahmen der Digitalisierung und der Industrie 4.0 zunehmend an Wichtigkeit gewinnen.

Durch den Einsatz von Blockchain-Technologien können KMU diesen Herausforderungen effizient begegnen. Blockchain-Technologien erlauben die Bereitstellung konsistenter und verlässlicher Informationen über die gesamte Wertschöpfungskette hinweg. Die infolgedessen erreichbare stärkere Vernetzung zwischen den einzelnen Akteuren kann auch zukünftig die Beherrschbarkeit und zielgerichtete Steuerung dynamischer Wertschöpfungsnetzwerke sicherstellen. Die dezentrale Datenhaltung bildet zudem die Grundlage für Dateninfrastrukturen, welche eine Dezentralisierung der Unternehmenssteuerung ermöglichen.

Die entwickelte DIN SPEC schafft einen Standard und stellt Basiswissen über Blockchain-Applikationen für Unternehmen zur Verfügung. Der wissenschaftlich-technische Nutzen besteht in der Bereitstellung eines Gestaltungsleitfadens, anhand dessen die anwendenden Unternehmen die Anforderungen an Blockchain-Applikationen ohne Expert:innenwissen herausarbeiten können. Anschließend befähigt der Leitfaden die Implementierung der entsprechenden Blockchain-Applikationen im Unternehmen.

Aus wirtschaftlicher Sicht bietet die Anwendung und Entwicklung von Blockchain-Technologien im Supply-Chain-Management besonderes Innovationspotenzial. Durch die fehlende Notwendigkeit eines Intermediärs wird eine höhere Datensicherheit erreicht und Kosten können gespart werden. Weiterhin wirkt sich ein höherer Informationsaustausch positiv auf die Performance der Supply-Chains aus und stellt so einen direkten Wettbewerbsvorteil dar. Schließlich wird durch eine präzisere Produktrückverfolgung und höhere Transparenz in den Lieferketten eine ressourcenschonendere Wertschöpfung ermöglicht. Durch die Anwendung des Gestaltungsleitfadens können diese Potenziale in KMU erfolgreich realisiert werden.

Es wurden Gestaltungsempfehlungen entwickelt, welche die Anwendung der Forschungsergebnisse in der Praxis sicherstellen und erleichtern soll.

4 Fortschreibung des Ergebnistransfers und Einschätzung der Realisierbarkeit des Transferkonzepts

Der Wissenstransfer der aus dem Forschungsprojekt gewonnenen Erkenntnisse in die Wirtschaft wurde sowohl projektbegleitend als auch abschließend durchgeführt.

Der Transfer wurde zum einen durch regelmäßige Treffen mit den Unternehmen des projektbegleitenden Ausschusses sichergestellt. So fanden insgesamt drei Treffen unter der Beteiligung der Unternehmen statt, bei denen die neuesten Erkenntnisse und Ergebnisse vorgestellt wurden. Nach dem dritten pbA-Treffen traf sich der projektbegleitende Ausschuss im Zuge der DIN-SPEC-Erstellung weitere fünf Mal. Zum anderen wurden die erarbeiteten Projektergebnisse zusätzlich bei verschiedenen Veranstaltungen und Veröffentlichungen an industrielle Partner weitergegeben (vgl. nachfolgende Tabellen).

Für die Realisierbarkeit des Transferkonzepts ist mit der gründlichen Erstellung des Standards im Rahmen der inhaltlichen Arbeitspakete ein wichtiger Grundstein für den Transfer der Ergebnisse nach Projektende gelegt worden. Durch die enge Zusammenarbeit mit den relevanten industriellen Partnern (s. insbesondere AP 2) wurde zudem eine direkte Anwendbarkeit sichergestellt. Zusätzlich sind die Erkenntnisse in Form des Gestaltungsleitfadens, welcher die Vor- und Nachteile der einzelnen Lösungsbausteine darlegt und diskutiert, durch ihre anwenderfreundliche Struktur direkt nutzbar. Dies bestätigte sich in der Validierung (s. AP 6). Hierbei sei angemerkt, dass es sich bei dem anonymen Herstellerunternehmen um ein Unternehmen außerhalb des projektbegleitenden Ausschusses handelt, was wiederum die mögliche breitenwirksame Validierung untermauert. Außerdem ist noch hervorzuheben, dass die DIN SPEC 32790 („Referenzarchitektur für Blockchain-Applikationen zur Schaffung von Transparenz in Supply-Chains“) die Implementierung von Blockchain-Lösungen vereinfacht. Dadurch können zum einen Unternehmen die für sie passenden Lösungen einfacher auswählen und zum anderen werden die für KMU bedeutsamen Schnittstellenproblemen und Eintrittsbarrieren signifikant reduziert.

Durchgeführte und geplante Transfermaßnahmen während des Projektzeitraums

Maßnahme	Ziel	Beschreibung der Maßnahme zum Ergebnistransfer	Datum / Zeit
Treffen mit dem projektbegleitenden Ausschuss	Absicherung der Praxis-tauglichkeit der Ergebnisse	1. PA-Treffen (Kick-off)	03.09.2020
		2. PA-Treffen	12.04.2021
		3. PA-Treffen	08.09.2021
		4. PA-Treffen / DIN-SPEC-Workshop	18.01.2022
		5. PA-Treffen / DIN-SPEC-Workshop	23.02.2022
		6. PA-Treffen / DIN-SPEC-Workshop	21.03.2022
		7. PA-Treffen / DIN-SPEC-Workshop	26.04.2022
		8. PA-Treffen / DIN-SPEC-Workshop	01.08.2022
Veranstaltungen mit Industrievertretern am Cluster Smart Logistik in Aachen	Führungskräfte aus verschiedenen Branchen über das Thema informieren	DDIM.kongress	19.11.2021
		Online-Seminar beim FBDi	01.12.2021
Organisation von Veranstaltungen	Austausch mit KMU	Workshop zur Identifikation von relevanten Schnittstellen (23 Teilnehmende)	02.11.2021
Wissenschaftliche Publikationen	Wissenschaftliche Diskussion der Ergebnisse	UdZForschung	01.12.2020
		Logistik Heute	19.05.2021
Präsentation auf Fachtagungen, Messen, Konferenzen	Verarbeitung von Ergebnissen für die nationale/internationale Fachwelt	Congress on Business Applications 2021	23.06.2021
Präsentation der Projektergebnisse	Bekanntmachung der Projektergebnisse, direkte Gesprächsmöglichkeiten für Interessierte	Internetveröffentlichung bei Roland Berger (<i>Blockchain Innovation Circle</i>)	28.05.2021
Präsenz im Internet	Bekanntmachung des Projekts / der Ergebnisse	FIR-Webseite	05.07.2021
		DIN-Webseite	06.01.2022
		Publikations-Webseite (epub.fir.de)	16.08.2022
Begleitung in universitärer Lehre	Vermittlung der Projekthalte und wissenschaftlicher Arbeit	Betreuung Bachelorarbeit	15.03.2021
		Betreuung Bachelorarbeit	05.05.2021

Tabelle 9: Ergebnistransfer während der Projektlaufzeit

Zusätzlich zu den durchgeführten Transfermaßnahmen sind noch einige Transfermaßnahmen im Anschluss an das Forschungsprojekt geplant.

Geplante Transfermaßnahmen nach dem Projektzeitraum

Maßnahme	Ziel	Beschreibung der Maßnahme zum Ergebnistransfer	Datum / Zeit
Ergebnisverwertung am FIR	Projektergebnisse weiterentwickeln, Öffentlichkeit zugänglich machen	Überführung der Ergebnisse in die Weiterentwicklung des Themenschwerpunkts Supply-Chain-Data-Management	laufend, seit 03/2022
Darstellung der Erkenntnisse	Anfass- und Begreifbar machen der Ergebnisse	Einbindung der Projektergebnisse in Führungen des Themenparks (ca. 15.000 Besucher/Jahr) und Future Logistics	laufend seit 09/2022
Veröffentlichung von Architektur / Standards / Normen etc.	Austausch mit KMU	Veröffentlichung DIN SPEC	01.11.2022
Präsentation der Projektergebnisse	Wissenschaftliche Diskussion der Ergebnisse	Roundtable Supply-Chain-Management	27.10.2022
Integration in Weiterbildungsprogramme	Verarbeitung von Ergebnissen an die nationale/internationale Fachwelt	Einbindung in den Zertifikatskurs Supply-Chain-Management (Einheit Supply-Chain-Data-Management)	laufend, seit 09/2022
Integration in Lehrangebot	Bekanntmachung der Projektergebnisse, direkte Gesprächsmöglichkeiten für Interessierte	Einbindung in Industrielle Logistik (Einheit Supply-Chain-Data-Management)	laufend, seit WS 2022/23
		Einbindung in Produktionsmanagement II (Einheit Supply-Chain-Management)	laufend, seit WS 2021/22

Tabelle 10: Ergebnistransfer nach dem Projektzeitraum

Literaturverzeichnis

- BADEV, A. I; CHEN, M.: Bitcoin: Technical Background and Data Analysis. FEDS Working Paper No. 2014-104. In: SSRN Electronic Journal (2014) 104, S. 1–38.
- BERGHOFF, C; GEBHARDT, U; LOCHTER, M; MAßBERG, S.: Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen. Bonn, März 2019. https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3
(Link zuletzt geprüft: 24.03.2023)
- FISCHER, P; HOFER, P.: Lexikon der Informatik. 15., überarb. Auflage. Springer, Berlin [u. a.] 2011.
- FUßWINKEL, O.; KREITERLING, C.: Beiträge aus den BaFinPerspektiven – Blockchain-Technologie – Gedanken zur Regulierung. BaFin online, 01.08.2018. https://www.bafin.de/Shared-Docs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html
(Link zuletzt geprüft: 24.03.2023)
- GAO, Z; XU, L; CHEN, L; ZHAO, X; LU, Y; SHI, W.: CoC: A Unified Distributed Ledger Based Supply Chain Management System. In: Journal of Computer Science and Technology 33 (2018) 2, S. 237–248.
- HAMADI, E. B.: [Conference Paper] Blockchain for Enterprise: Overview, Opportunities and Challenges. The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017), Juli 2017, Nice, France. http://personales.upv.es/thinkmind/dl/conferences/icwmc/icwmc_2017/icwmc_2017_5_10_28001.pdf (Link zuletzt geprüft: 24.03.2023)
- HEPP, T; SHARINGHOUSEN, M; EHRET, P; SCHOENHALS, A; GIPP, B.: On-chain vs. off-chain storage for supply- and blockchain integration. In: it - Information Technology 60 (2018) 5–6, S. 283–291.
- Hermes Germany GmbH (Hrsg.): Nachhaltigkeit im Supply Chain Management. Die 12. Ausgabe des Hermes-Barometers präsentiert die Ergebnisse einer Telefonbefragung unter rund 200 Logistikentscheidern in Deutschland. Hamburg, April 2020. <https://www.hermes-supply-chain-blog.com/wp-content/uploads/2020/04/Hermes-Barometer-12-Nachhaltigkeit-im-SCM.pdf> (Link zuletzt geprüft: 24.03.2023)
- HOLTKEMPER, D.: Blockchain-Applikation für das Supply-Chain-Management. Schriftenreihe Rationalisierung; Bd. 170. RHRsg.: G. Schuh. Apprimus, Aachen 2020. – Zugl.: Aachen, Techn. Hochsch., Diss., 2020.
- LU, T; GUO, X; XU, B; ZHAO, L; PENG, Y; YANG, H.: Next Big Thing in Big Data: The Security of the ICT Supply Chain. In: 2013 International Conference on Social Computing. Ed.: International Conference on Social Computing. IEEE 08.09.2013 – 14.09.2013, S. 1066 – 1073.

Direktlink zum PDF: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6693469>
(Link zuletzt geprüft: 24.03.2023) DOI: 10.1109/SocialCom.2013.172

MEIER, A.: Blockchain-Voting für MyPolitics und OurPolitic. In: Blockchain. Grundlagen, Anwendungsszenarien und Nutzungspotenziale. Hrsg.: H.-G. Fill; A. Meier. Springer Vieweg, Wiesbaden 2020, S. 337 – 354.

RODENHÄUSER, B; RAUCH, C.: Supply Chain 2025. Eine Studie des Zukunftsinstituts für den Verband der Wellpappen-Industrie. Zukunftsinstitut GmbH, Frankfurt am Main 2015. [in Bibliothek des FIR e. V. an der RWTH Aachen verfügbar]

SCHLATT, V; SCHWEIZER, A; URBACH, N; FRIDGEN, G.: [Discussion Paper] Blockchain: Grundlagen, Anwendungen und Potenziale. Fraunhofer FIT, Dezember 2016. <https://fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf> (Link zuletzt geprüft: 24.03.2023)

SCHUH, G; ANDERL, R; GAUSEMEIER, J; HOMPEL, M. ten; Wahlster W. (Hrsg.): Industrie 4.0 Maturity Index. Die digitale Transformation von Unternehmen gestalten. acatech, München, April 2017. <https://www.acatech.de/publikation/industrie-4-0-maturity-index-die-digitale-transformation-von-unternehmen-gestalten/download-pdf?lang=de> (Link zuletzt geprüft: 24.03.2023)

SHAH, K.; SHAH, N.; SHAH S.; PATEL, D.: Email User Classification and Topic Modeling. In: Proceedings of the Future Technologies Conference (FTC) 2020; Vol. 1. Advances in intelligent systems and computing; Bd. 1289. Springer, Cham [u. a.] 2021, S. 359–377.

SIEGEL, D.: Blockchain – Begriff, Potenziale, Bewertung. In: WiSt – Wirtschaftswissenschaftliches Studium 46 (2017) 12, S. 45–47.

SORGE, C; KROHN-GRIMBERGHE, A.: Bitcoin – das Zahlungsmittel der Zukunft? In: Ökonomische Trends 93(2013)10, S. 720 – 722. <https://www.wirtschaftsdienst.eu/inhalt/jahr/2013/heft/10/beitrag/bitcoin-das-zahlungsmittel-der-zukunft.html> (Link zuletzt geprüft: 24.03.2023)

WUST, K; GERVAIS, A.: Do you Need a Blockchain? <https://eprint.iacr.org/2017/375.pdf> (Link zuletzt geprüft: 24.03.2023)