DISTRIBUTED LEDGER TECHNOLOGIES IN LOGISTIK UND SUPPLY CHAIN MANAGEMENT IM KONTEXT VON DATENSICHERHEIT UND DATENQUALITÄT

Maximilian Stange
Fraunhofer Institut für Werkzeugmaschinen und Umformtechnik IWU,
Reichenhainer Straße 88, D-09126 Chemnitz

In der Anfangszeit der Distributed Ledger Technologies (DLT) waren die hauptsächlichen Betrachtungswinkel die der Disruption des Bank- und Finanzwesens. Mit dem Aufkommen des Systems Ethereum im Jahr 2015, hat die Auseinandersetzung mit der Anwendung von Blockchain in weiteren Branchen, an Bedeutung gewonnen. Eine davon ist die Logistik und das Supply Chain Management (SCM). Gerade in Deutschland spielt der Logistiksektor eine große Rolle, nach der Beschäftigtenzahl ist er die drittgrößte Branche und erzielt einen Umsatz von rund 258 Milliarden Euro. Im Beitrag werden konkrete Anwendungsfelder identifiziert und gezeigt welche potentiellen Vorteile sich dort, durch den Einsatz von DLT, erzielen lassen. Ein Schwerpunkt liegt dabei auf der Einschätzung der Technologie hinsichtlich ihrer Sicherheitseigenschaften. Im Beitrag wird den Fragen nachgegangen, ob Datensicherheit mithilfe von DLT verbessert werden kann und auf welchem Wege.

1. Einleitung

Bitcoin hat es im Jahr 2017 geschafft der breiten Öffentlichkeit ein Begriff zu werden. Das liegt vor allem an der enormen Wertsteigerung, die die Kryptowährung zu einem begehrten Investment gemacht haben. Die den Kryptowährungen zugrundeliegende Technologie ist als Blockchain bekannt. Sie ist, vereinfacht ausgedrückt, „ein Medium für digitale Werte“, das diese durch kryptografische Verfahren schützt.

Anhand des Aufkommens von digitalen Währungen ist ersichtlich, dass ein großes Potential besteht, die Finanzbranche grundlegend umzuwälzen. Aber auch andere Branchen stehen, aufgrund der Technologie, vor einem Wandel. Dabei werden immer wieder die Bereiche Logistik und SCM genannt. Gerade in Deutschland spielt der Logistiksektor eine große Rolle, nach der Beschäftigtenzahl ist er die drittgrößte Branche und erzielt einen Umsatz von rund 279 Milliarden Euro [1].

Ein Beispiel für die Anwendung in diesem Bereich ist die Rechnungsstellung. Derzeitige Warenwirtschaftssysteme erfassen heute in Sekundenbruchteilen Änderungen im Bestand bei einer Bestellung. Die Rechnungsstellung findet aber oft noch manuell statt und dauert dementsprechend länger. Es ist denkbar diesen Prozess mithilfe eines Smart Contracts zu automatisieren und somit zu beschleunigen, womit beispielsweise die Liquidität einer Unternehmung erhöht werden kann. Daneben existieren eine Reihe weiterer angedachter Anwendungen von DLT in der Branche, die zum Teil auch auf Smart Contracts basieren. Diese sollen hier aufgezeigt und deren Potential abgeschätzt werden. Ein Schwerpunkt liegt dabei auf der Einschätzung der Technologie hinsichtlich ihrer Sicherheitseigenschaften. Denn das Thema IT-Sicherheit gewinnt immer mehr an Bedeutung, gerade im Hinblick auf die gleichbleibend hohe Gefährdungslage im Bereich der Cyberspionage zu Ungunsten deutscher Unternehmen [2].

2. Begriffseinordnungen

Distributed-Ledger-Technologien stellen ein relativ neues Forschungsfeld dar, daher gibt es auch keine einheitliche Definition und verschiedene technische Ausführungen werden darunter subsumiert [3]. Verallgemeinert handelt es sich um Systeme zur verteilten Kontoführung, bei denen die Daten von allen, oder zumindest mehreren Computern im beteiligten Netzwerk genutzt, weitergegeben und verifiziert werden [4]. Hauptmerkmale von DLT sind:

a) Im Vergleich, zu den bisher üblichen Shared-Ledgers sind Distributed-Ledger-Systeme nicht auf eine übergeordnete, zentrale Instanz angewiesen. Informationen in digitaler Form können zwischen Parteien, die sich untereinander nicht vertrauen, ausgetauscht und gespeichert werden.

b) DLT stellen sicher, dass es zu keinem Double-Spending kommen kann. Double Spending bezeichnet dabei das mehrfache Ausgeben eines digitalen Guts beispielsweise eines Bitcoins.

Allgemein ausgedrückt werden DLT dazu genutzt den Besitz von digitalen Gütern nachzuverfolgen. Beispiele für DLT sind das Bitcoin- und das Ethereum-Netzwerk.

Smart Contracts (SC) können, wenn sie mithilfe einer DLT implementiert wurden, als unveränderliche Computerprogramme bezeichnet werden, die „rechtlich relevante Handlungen […] in Abhängigkeit von digital prüfbaren Ereignissen steuer[n], kontrollier[en] und/oder dokumentier[en] […] [5].

Smart Contracts, die für ihre Ausführung auf Informationen außerhalb der Blockchain angewiesen sind, werden als **non-deterministic Smart Contracts** (NDSC) bezeichnet. Diese Art von Smart Contracts erweitert das Spektrum an möglichen Anwendungsszenarien beträchtlich [6]. Ihr Einsatz birgt jedoch auch Gefahren, da hier der Rückgriff auf Daten einer dritten Partei nötig ist, die nicht in jedem Fall fehlerfrei agiert und nicht immer völlig vertrauensvoll ist. Dem gegenüber stehen sogenannte **deterministic Smart Contracts** (DSC). DSC sind solche Smart Contracts die nur aufgrund der Informationen, die in dem DL

vorhanden sind funktionieren.

Da eine direkte Anbindung an eine externe Datenquelle (z.B. ein aktueller Börsenkurs) einen nicht deterministischen Zustand des Ledgers auslösen könnte, werden **Oracles** als vermittelnde Instanz verwendet. Grundsätzlich sind Oracles auch Smart Contracts. Sie dienen lediglich als vermittelnde Instanz zwischen externen Datenquellen und anderen Smart Contracts. Smart Contracts, die auf externe Informationen angewiesen sind, um zu funktionieren, fragen ein Oracle ab, anstatt dies direkt bei der originären Datenquelle zu tun. Dafür sendet die externe Datenquelle dem Oracle Updates über den abzufragenden Zustand, dadurch werden Inkonsistenzen vermieden, da nun ein Smart Contract einen anderen abfragt [7]. Das bedeutet, dass das an sich geschlossene System eines Distributed Ledgers durch Oracles um eine Anbindung an die Außenwelt erweitert wird, was die Nutzung externer Datenquellen erlaubt.

3. Anwendungsfelder von Smart Contracts

Die Anwendungsfelder von Smart Contracts werden durch die Vorteile definiert, die diese Technologie mit sich bringt. Zu den größten Vorteilen von Smart Contracts gehören:

- Sehr geringe Wahrscheinlichkeit, dass die in den Smart Contract festgelegten Vereinbarungen nicht durchgesetzt werden → Durch die dezentrale Ausführung und Validierung des Smart Contracts
- Genauigkeit → z.B. Reduzierung der Fehlerquote, dort wo sonst manuell Daten übertragen werden
- Höhere Geschwindigkeit durch Automatisierung von bisher manuellen Prozessen → z.B. Vergleich mehrerer Quellen ob ein Flugzeug Verspätung hat und sofortige Freigabe der Versicherungssumme, sollte der Versicherungsfall eintreten.
- Reduzierung der Zahl an Intermediären → Vertrauen unter den Vertragsparteien ist nicht nötig, daher werden Dritte, die für die Einhaltung von vertraglichen Vereinbarungen garantieren, nicht benötigt
- Geringere Kosten → Durch die vorher genannten Punkte [8]

Use Cases für Smart Contracts sind somit dort zu finden, wo die Digitalisierung und Automatisierung von Prozessen bisher, aufgrund des Fehlens fälschungssicherer digitaler Dokumente, nicht möglich war. Neben der Prozessoptimierung werden durch Smart Contracts auch gänzlich neue Geschäftsmodelle möglich. Decentralized Autonomous Organizations (DAO) sind ein Beispiel für ein neues Geschäftsmodell auf Basis von Smart Contracts. DAOs sind Organisationen ohne Vorstände und Geschäftsführer, die sich selbst verwalten und in denen Nutzer Stimm- und Eigentumsrechte erwerben können, um beispielsweise über zukünftige Investitionen zu bestimmen [9].

4. Limitierungen von Smart Contracts

Die zuvor genannten Vorteile der Smart Contracts lassen sich aufgrund von Limitierungen hinsichtlich der Sicherheit, Anwendbarkeit und weiterer Faktoren, noch nicht in umfänglicher Weise in reale Anwendungen übertragen beziehungsweise verhindern deren Ausdehnung auf größere Benutzergruppen.

Zu den gewichtigsten Faktoren, die den Einsatz von Smart Contracts hemmen, gehören problematische Aspekte bei der Sicherheit von Smart Contracts. Eine vollumfängliche Darstellung gibt es auch hier noch nicht, unter anderem wegen der noch geringen Verbreitung von Smart Contracts [7]. Trotzdem ist bereits bekannt, welche gravierenden Folgen durch Sicherheitslücken entstehen können. Bekanntestes Beispiel dafür ist die bereits angesprochene DAO, eine Investmentfirma ohne menschliches Personal. Durch einen Programmierfehler wurden digitale Token im Wert von 53 Millionen Dollar entwendet. Nur durch eine Protokolländerung (Hard Fork) der gesamten Ethereum-Blockchain konnte der Schaden rückgängig gemacht werden. Dadurch existiert aber seitdem neben Ethereum noch die Kryptowährung Ethereum Classic [10].

Eine der ersten Publikationen zur Sicherheit von Smart Contracts auf Basis von Ethereum stammt von DELMOLINO ET AL. (2016) und bezieht sich auf die Besonderheiten in der Programmierung von Smart Contracts und häufig begangenen Fehlern, die auf die Eigenheiten von DL zurückzuführen sind.

Im Wesentlichen stellen sie drei Fehlerarten fest:

1. Smart Contracts, die gesendeten Beträge einschließen und nicht wieder freigeben
2. Speichern von Nutzerinformationen in Klartext, wodurch eine andere Partei einen Vorteil erzielen kann
3. Falsch gesetzte Anreize können dazu führen, dass sich Nutzer nicht wie beabsichtig verhalten, da ein Fehlverhalten nicht oder nicht stark genug bestraft wird [11].

LUU ET AL. (2016) zeigen mit ihrem Tool Oyente, dass 45 % aller Smart Contracts in Ethereum nach ihrer Definition Bugs besitzen, die von Angreifern ausgenutzt werden könnten [12]. Die meisten Fehler treten dabei bei der Behandlung von Ausnahmen auf. Das kann unter anderem dazu führen, dass Gelder unwiderruflich in einem Smart Contract verbleiben, ohne dass der rechtmäßige Besitzer darauf Zugriff erhält [12].

NIKOLIC ET AL. (2018) definieren in ihrer Untersuchung drei Arten angreifbarer Contracts:

Verschwenderische Smart Contracts → Sind solche Verträge, die Gelder willkürlich an andere Adressen schicken können.

1. Suizidale Smart Contracts → Können von anderen Nutzern als dem Ersteller oder an-deren berechtigten Personen zerstört werden.
2. Gierige Smart Contracts → Behalten eingezahlte Gelder ein, ohne dass eine Möglichkeit besteht

sie wieder freizugeben [13].

Von knapp einer Million untersuchter Smart Contracts können rund 2,5 % in einer der von den Autoren definierten Kategorien eingeordnet werden. Die Diskrepanz zwischen den Zahlenangaben zu Smart Contracts mit sicherheitsrelevanten Schwachstellen (45% zu 2,5 %) zeigt, dass einheitliche Bewertungsmaßstäbe gefunden werden müssen. Beide Untersuchungen zeigen jedoch unabhängig davon, dass ein nicht vernachlässigbarer Anteil von Smart Contracts über potentiell gefährliche Fehler verfügt, die die Gelder von Nutzern gefährden. Eine Lösung hierfür ist die Überprüfung von Smart Contracts mit den von den Autoren entwickelten Tools, bevor sie eingesetzt werden, um solche Sicherheitslücken zu vermeiden. Natürlich gibt es auch in jeder anderen Software Bugs, Anwendungen auf Basis von DLT sind jedoch durch drei Eigenschaften besonders gefährdet:

1. **Finalität von Transaktionen**
   Eigentlich ein Vorteil von Distributed Ledgers, jedoch können beispielweise bei einer erfolgreichen Attacke die Beträge nicht zurückgebucht werden oder ähnliches. Nur durch die Änderung des gesamten Protokolls, der alle Knoten zustimmen müssen kann eine Entschädigung stattfinden. Im Falle von The DAO wurde dies nur durchgeführt, da ein großer Anteil von Ether in The DAO investiert wurde, dadurch war die Anwendung „too big to fail“ [10]. Für Smart Contracts mit kleineren Summen ist diese Art der Rettung so gut wie ausgeschlossen. Aber auch Hacks und Bugs, deren Größenordnung, gemessen an den involvierten Summen an Kryptowährungen, die des DAO-Hacks übersteigen, können nicht grundsätzlich auf eine Rettung hoffen. Beispiel hierfür ist der als Parity Bug bzw. Hack bezeichnete Fall, indem die Gelder einer Wallet Software nicht mehr zugänglich waren, da ein unberechtigter Nutzer eine notwendige Bibliothek gelöscht hatte (Suizidaler Smart Contract).
2. **Starker monetärer Anreiz Smart Contracts anzugreifen**
   Da fast die Hälfte aller Smart Contracts Finanzgeschäfte abwickeln und somit Kryptowährungen verwalten, ist der potentielle finanzielle Gewinn eines Angriffes hoch.
3. **Noch keine Rechtssicherheit**
   Fehlende Regulierung im Bereich der DL erhöht das Risiko für Nutzer im Falle eines Angriffs keine Entschädigung außerhalb der DL-Infrastruktur zu erhalten etwa über ein Gerichtsverfahren.

5. Problematik Oracles

Die Probleme, welche sich mit der Nutzung von Oracles auftun, sind offensichtlich, da sie die Zielsetzungen von DL konterkarieren zu scheinen. Distributed Ledger werden genutzt, um revisionssichere Transaktionen durchzuführen, ohne dass sich die Teilnehmer untereinander vertrauen. Wird jedoch für ein Smart Contract ein Oracle genutzt, das die Daten aus einer externen Quelle bezieht wird Vertrauen wieder nötig [14]. Zum einem Vertrauen in die Validität der Daten aus der externen Quelle, zum anderen Vertrauen darin, dass die Daten vom eingesetzten Oracle nicht verändert wurden.

Allgemein, sind die als CIA-Triade bezeichneten Begriffe, confidentiality (Vertraulichkeit), integrity (Integrität) und availability (Verfügbarkeit), ein fundamentales Modell für Betrachtungen in der Computersicherheit, auch für Smart Contract Oracles gültig. Vertraulichkeit steht für den Schutz, dass Daten nicht unautorisiert veröffentlicht werden. Integrität ist der Schutz vor der unerlaubten Änderung von Daten und Verfügbarkeit bezeichnet den Schutz vor unautorisierter Dienstverweigerung (beispielsweise durch Distributed-Denial-of-Service-Attacken) [15]. Oracles können diese Eigenschaften ohne zusätzliche Maßnahmen nur schlecht erfüllen. Dieses konzeptionelle Problem, sich widersprechender Eigenschaften von Smart Contracts und Oracles, ist ein in der Forschung und Industrie bekanntes.

Ein Ansatzpunkt den Widerspruch aufzulösen ist die Nutzung von externen Quellen denen ohnehin vertraut wird, beziehungsweise denen vertraut werden muss. Anwendungen die beispielsweise die Validierung von staatlichen Stellen benötigen, können und müssen von eben diesen mit Daten in Form von Oracles gespeist werden, womit keiner zusätzlichen Entität vertraut werden muss [16]. Dies ist jedoch nur für eine begrenzte Anzahl von Anwendungen der Fall und mit Hinblick auf die Zielsetzung von DL, dass sichere Transaktionen zwischen Parteien abgewickelt werden sollen, die sich nicht vertrauen, auch keine primäre Anwendung.

ZHANG ET AL. (2016) setzen für das Problem der sicheren und nicht manipulierten Übertragung von Daten, von externen Quellen zu einem Oracle auf ein von ihnen entwickeltes Protokoll mit dem Namen Town Crier [17]. Town Crier setzt hierbei stark auf die Nutzung von Software Guard Extensions von Intel, wie auch der Konsensmechanismus Proof of Elapsed Time, um Code in einer sicheren Umgebung auszuführen. Dadurch soll die Authentizität und Integrität der Daten eines Oracles sichergestellt werden. Daneben soll durch die Verschlüsselung von so genannten „datagrams“ Vertraulichkeit in den Abfragen an ein Oracle gewährleistet werden. Dies ist insofern wichtig, weil in einem öffentlichen DL alle Transaktionen für jeden Teilnehmer einsehbar sind. Für viele Anwendungen ist jedoch ein gewisser Grad an Vertraulichkeit notwendig.

Ein weiterer Ansatz, der zum Beispiel von der Firma ChainLink angewandt wird, ist die Verteilung von Datenquellen und Oracles. Einfach ausgedrückt, werden für ein Oracle verschiedene Datenquellen genutzt und deren Ergebnisse zu einer Abfrage aggregiert, weitere Oracles mit teilweise anderen Datenquellen führen auch eine Abfrage durch und aggregieren die Ergebnisse. Die Ergebnisse aller Oracles werden am Ende ebenfalls aggregiert und bilden somit den Input für den Smart Contract, der einen bestimmten Parameter abfragt [18].

Mithilfe aller dieser Ansätze lassen sich Risiken in der Nutzung von Oracles für Smart Contracts minimieren. Jedoch kann, durch die ständige Weiterentwicklung des Feldes, noch kein abschließendes Urteil zur Sicherheit von Oracles getroffen werden.

6. Anwendung von DLT in Logistik und SCM

Nachdem in den vorherigen Abschnitten aufgezeigt wurde, wo die Potentiale von DLT liegen, aber auch ihre Limitierungen, soll geprüft werden, wo diese Technologien in Logistik und SCM angewandt werden. Dazu wurden 37 verschiedenen Case Studies bzw. Projekte ausgewertet, die alle öffentlich zugänglich sind. Die Anwendungsbereiche wurden in sechs Kategorien zusammengefasst. Diese sind in Tabelle 1 zusammengefasst.

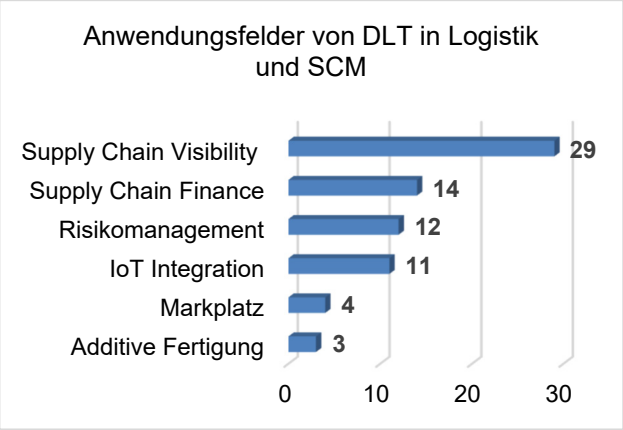

Abbildung 1 - Anwendungsfelder von DLT in Logistik und SCM

Die Case Studies und Projekte wurden zu denen in Tabelle 1 definierten Anwendungsfeldern zugeordnet. Eine Mehrfacheinordnung wurde teilweise vorgenommen. Die Ergebnisse sind in Abbildung 1 zu sehen. Das Anwendungsfeld Supply Chain Visibility, worunter auch das Tracking und Tracing fällt ist dominant in der Anwendung der DLT im SCM. Supply Chain Finance folgt mit deutlichem Abstand, was überraschend ist, da die ganze Technologie als ein neuartiges Finanzinstrument gestartet ist und in vielen Berichten primär auch noch als dieses gesehen wird. Die Integration von IoT-Geräten und Sensoren sowie Risikomanagement sind weiterhin wichtige Anwendungsfelder. Marktplätze für logistische Dienstleistungen und die Integration in die Additive Fertigung stellen derzeit Nischenanwendungen dar.

Kategorie	Supply Chain Visibility	Supply Chain Finance
Merkmale	Tracking und Tracing	Digitalisierung von Frachtdokumenten
	Herkunftsnachweise für Kunden und Endverbraucher und Behörden	Automatische Abwicklung von Zahlungen über Token, Kryptowährungen und Smart Contracts
	Audits	Know Your Customer
	Bestandsmanagement	
Kategorie	**IoT Integration**	**Additive Fertigung (AF)**
Merkmale	Integration von IoT Geräten und Sensoren zur Datenerfassung & Automatisierung	Sichern der Datenübertragung in der AF + Herkunfts-nachweise in DLT
Kategorie	**Risikomanagement**	**Marktplatz**
Merkmale	Reaktionsvermögen durch besseren Zugriff auf Daten	Sicherer Marktplatz zum Handel von Gütern und Dienstleistungen
	Sichere Qualitätsnachweise der Lieferanten	Automatische Verhandlungen M2M
	Einfachere Streitlösung	
	Schutz vor Produktfälschungen	

Tabelle 1 - Kategorisierung der Anwendungsfelder von DLT in SCM und Logistik

Daneben wurde den untersuchten Fällen ein Anwendungsbereich zugeordnet. Die Ergebnisse sind dazu in Abbildung 2 zusammengefasst.

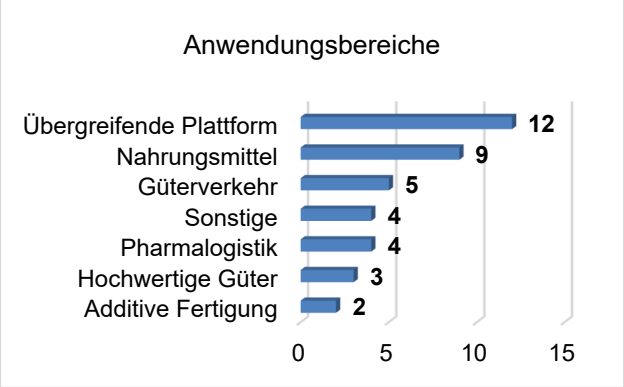

Abbildung 2 - Anwendungsbereiche von DLT in Logistik und SCM

Eine Branche in der der Einsatz von DLT stark diskutiert wird, ist die Nahrungsmittelbranche. Hier geht es primär darum das Vertrauen der Verbraucher, das durch die zahlreichen Lebensmittelskandale stark gelitten hat, wieder zu gewinnen. Sichere Herkunftsnachweise sollen den Verbrauchern eine Garantie über die Quelle ihrer Produkte geben und zwar über die ganze Supply Chain hinweg. Eine ähnliche Thematik spielt für die Anwendung in der Pharmalogistik eine Rolle. Auch hier gab es in den vergangenen Jahren Skandale gerade in Asien. Weitere Anwendungsbereiche sind der Güterverkehr und die Herstellung und Handel mit hochwertigen Gütern, worunter beispielsweise die Firma Everledger fällt, die Diamanten registriert.

In den Case Studies häufig genannte Vorteile von DLT in Logistik und SCM waren: höhere Transparenz, Sichere Herkunftsnachweise, Erhöhung von Datensicherheit und -integrität, Prozessautomatisierungen, Kostensenkungen.

Um die in den Case Studies identifizierten Vorteile weiter zu untersetzen, wird ein Literature Review durchgeführt.

7. Literature Review

Als Grundlage der eigenen Methodik dienen die Ausführungen von DURACH ET AL. (2017), die Literature Reviews im Bereich der Forschung zum Supply Chain Management systematisierten [19]. Im ersten Schritt der Methode geht es um die möglichst konkrete Formulierung der Forschungsfragen. Die vordergründig zu beantwortenden Forschungsfragen sind hierbei:

1. Welche Vorteile werden durch den Einsatz von DLT erzielt und wie sind sie quantifizierbar?
2. Welche Implikationen ergeben sich daraus auf die Datensicherheit im Speziellen und die Sicherheit der Unternehmung im Allgemeinen, beispielsweise bezogen auf die Einhaltung rechtlicher Vorgaben?

Darauffolgend werden potentiell relevante Quellen durch eine Suche in einschlägigen Datenbanken ermittelt. Neben der bloßen Suche in den Datenbanken werden auch die Querverweise der ausgewählten Publikationen untersucht. Die Suchmethode orientiert sich dabei an den von DENYER UND TRANFIELD (2009) gemachten Angaben [20]. Gefundene Quellen werden anhand der in Schritt zwei bereits definierten Kriterien, entweder in die Untersuchung aufgenommen oder davon ausgeschlossen.

8. Vorteile durch DLT in Logistik und SCM

Im Bezug zu den Vorteilen, die durch DLT erreicht werden können, decken sich die Ergebnisse der Auswertung der wissenschaftlichen Quellen zum Großteil, mit denen aus der Auswertung der Case Studies. Die Ergebnisse sind dazu in Tabelle 3 festgehalten. Eine Quantifizierung der Vorteile, die durch DLT erbracht werden, findet sich jedoch in keiner Quelle.

Von vielen Autoren werden die Automatisierung von Prozessen und die Schaffung von Transparenz als die größten Vorteile der Implementierung von DLT gesehen. Die Automatisierung bezieht sich dabei vor allem auf Finanztransaktionen, Streitresolution und Dokumentation von Prozessen. Diese Prozesse benötigen heute noch viele manuelle Interventionen, da sie nicht digitalisiert ablaufen und papierbasierte Dokumente benötigen. Bei vielen Prozessen ist dies der Fall, weil digitale Dokumente noch nicht genügend Sicherheit gegenüber Manipulation und Vervielfältigung aufweisen. Digitale Originale werden jedoch durch DLT möglich und eröffnen so neue Nutzungsmöglichkeiten und Wege zur Automatisierung von Prozessen, welche in der Regel durch Kosteneinsparung und einer höheren Güte der Prozesse verbunden sind.

Ein Beispiel, dass die Fähigkeit von DLT, Prozesse zu automatisieren, gut beschreibt ist die Digitalisierung der Bill of Lading (BoL), die auch als Konnossement bezeichnet wird. STAHLBOCK ET AL. (2018) haben sich damit auseinandergesetzt [21].

Die BoL ist ein wichtiges Dokument im maritimen Warenverkehr. Ihre hauptsächlichen Funktionen sind: „Beleg des Erhalts oder Verschiffens von Gütern, Beweis eines abgeschlossenen Frachtvertrags und die Repräsentation des Besitzrechtes der Güter.“ [21]. Durch den letzten Punkt wird die Digitalisierung des Dokumentes erschwert, denn es stellt auch ein Wertpapier dar. Also muss sichergestellt werden, dass eine digitale Repräsentation dieses Dokuments nicht vervielfältigt werden kann, dass also nur ein digitales Original besteht.

Warum ist eine Digitalisierung sinnvoll? Durch die Involvierung vieler verschiedener Parteien, beim Transport von Seefracht, kann es dazu kommen, dass die BoL nicht immer dort ist, wo sie gerade benötigt wird, beispielsweise um Waren freizugeben, die am Zielort angekommen sind. So kann die BoL, die nicht vervielfältigt werden darf, noch bei der Hafenverwaltung sein, obwohl sie vom Zoll benötigt wird. Dadurch kann es zu Verzögerung beim Löschen der Ware kommen, was in der Regel zu finanziellen Einbußen führt (z.B. könnten empfindliche Nahrungsmittel verderben). Daneben ist eine BoL als Papierdokument fehleranfällig, sie könnte beispielsweise verloren gehen.

Eine digitale BoL muss einige Anforderungen erfüllen. Die digitale BoL muss einzigartig und übertragbar sein. Die Integrität der Dokumente muss sichergestellt sein und, es muss ein Mechanismus bestehen, mit dem der Besitz des Dokumentes nachgewiesen werden kann, nach Ende des Geschäfts muss das Dokument seine rechtliche Wirkung verlieren [21]. Diese Eigenschaften lassen sich mit DLT erreichen. Ein Nachweis über den Besitz des Dokumentes lässt sich beispielsweise von jedem Teilnehmer, beim Blick auf die Transaktionen im Ledger, nachvollziehen. Durch eine mit DLT digitalisierte BoL werden manuelle Schritte wie das Übergeben der BoL nach dem Festmachen des Schiffes an die jeweiligen Autoritäten unnötig. Sie könnte gleich bei der Einfahrt in den Hafen automatisch übermittelt werden. Somit könnten Wartezeiten vermieden und die Ware schneller gelöscht werden.

Weitere Anwendungen im Bereich der Automatisierung gehen stark auf die Abwicklung von Finanzflüssen ein. Ein Ziel im SCM ist die Integration von Waren-, Informations- und Zahlungsflüssen. Die Abwicklung von Zahlungsflüssen ist jedoch noch stark von den eigentlichen Warenflüssen entkoppelt. Wie bereits beschrieben ist dies vor allem auf die weitverbreitete Nutzung papierbasierter Dokumente zurückzuführen. Analog zum Beispiel der BoL sind in diesem Bereich auch Vorteile durch die Digitalisierung solcher Dokumente zu erzielen. Daneben entstehen durch die automatisierte Abwicklung von Zahlungsströmen, auch in M2M-Beziehungen, neue Ge-

schäftsmodelle, wie dezentralisierte autonome Organisationen oder P2P-Netzwerke zum Handeln von Gütern z.B. elektrische Energie aus privaten regenerativen Quellen.

Vorteile durch DLT	Anzahl	Quellen
Automatisierung	12	[21]; [26]; [27];[28]; [29];[30]; [31]; [32]; [33];[34]; [35];[36]
Transparenz (unternehmensintern)	8	[26]; [32]; [34]; [35]; [37]; [38]; [39]; [40]
Transparenz (extern für Endverbraucher)	5	[25]; [37]; [41]; [42]; [43]
Neue Geschäftsmodelle	4	[28]; [29]; [44];[45];
Kontrollebene in IoT-Systemen	3	[27]; [39]; [43]
Produktfälschungen verhindern	3	[39]; [42], [46]
Interoperabilität von Systemen	2	[38]; [47]
Besserer Zugang zu Finanzierungsinstrumenten für KMU	1	[31]

Tabelle 2 - Auswertung Literature Review Vorteile durch DLT

Ein letzter Punkt der Automatisierung beschreibt die Streitresolution. Mithilfe von Smart Contracts können Logiken festgelegt werden, nach denen Algorithmen zwingend handeln, ohne dass eine Partei darin eingreifen könnte. Ein Beispiel hierzu sind Smart Contracts, die die Kühlung eines Medikamentes überwachen, sollten die Temperaturen über einen vorher definierten Zeitraum, nicht eingehalten werden, muss der Logistikdienstleister dem Hersteller eine Entschädigung zahlen, da das Produkt möglicherweise nicht mehr verkäuflich ist. Mit Smart Contracts wird sichergestellt, dass die Entschädigung auch gezahlt wird, da diese eine Zahlung automatisch veranlassen können, sobald der gewünschte Transportzustand nicht mehr erfüllt wird. Verhandlungen mit dem Transportdienstleister über solche Entschädigungen sind dann nicht mehr nötig.

Die Erzielung von Transparenz in Supply Chains ist, laut der Auswertung der Literature Reviews, neben der Automatisierung der bestimmende Vorteil von DLT im SCM. Es kann grob zwischen dem Ziel nach der Schaffung von unternehmensinterner und von externer Transparenz unterschieden werden. Externe Transparenz bezieht sich dabei auf die Schaffung von Transparenz für den Endkonsumenten eines Produktes. Das heißt dem Kunden wird die Möglichkeit geboten die Herkunft seines Produktes und die Produktionsbedingungen nachzuvollziehen. Dies ist eine Möglichkeit, Vertrauen zwischen Unternehmen und Kunden aufzubauen und so die Kundenbindung zu stärken. Einher geht dieser Ansatz auch oft mit dem Ziel, Produktfälschungen zu verhindern, beziehungsweise zu erschweren, dadurch, dass sich nur genuine Produkte über eine Abfrage in einem DL verifizieren lassen.

Interne Transparenz bezieht sich ausschließlich auf das Unternehmensnetzwerk. Der Grund hierfür liegt in der Absicherung der Unternehmen hinsichtlich der Herkunft der von Lieferanten bezogenen Teile oder Rohstoffe. So ist ein wichtiger Ansatzpunkt im Risikomanagement, der ausschließliche Bezug von Teilen und Rohstoffen aus bekannten Quellen. Dass ein bestimmtes Teil tatsächlich von einem bestimmten Lieferanten stammt, lässt sich mithilfe von DLT anhand der getätigten Transaktionen leicht überprüfen.

Grundlegend bei fast allen der diskutierten Anwendungen ist eine Datenbasis aus vielen Sensoren und Geräten. Somit sind diese Anwendungen von einer primären IoT-Infrastruktur abhängig. Um diese sicherer zu machen werden DLT in einigen Publikationen als eine Art Kontrollinstanz gesehen, die Informationen bzw. Transaktionen validiert und diese Netzwerke so zusätzlich schützt. Somit sind IoT und DLT fundamentale Bausteine für eine Verbesserung der Visibility, des Risikomanagements und der Abwicklung von Zahlungsflüssen in Supply Chains.

9. Sicherheitsimplikationen

Der Einsatz von DLT wird oft unter dem Aspekt einer Verbesserung der Sicherheit diskutiert. Daher wurden die Quellen, die sich mit der Anwendung der Technologie beschäftigen, auch dahingehend untersucht, wie DLT eine erhöhte Sicherheit von Anwendungen erzielen und welche Punkte sich möglicherweise negativ darauf auswirken.

Das am häufigsten angebrachte Argument dafür, dass DLT mehr Sicherheit schafft, ist dass dadurch die Manipulierbarkeit von Daten stark reduziert wird oder sogar, mit vertretbaren Mitteln, ganz ausgeschlossen ist. Gerade in Bezug auf IoT-Geräte, die allzu oft leicht angreifbar sind und bei Finanztransaktionen, ist eine Verbesserung der Manipulationssicherheit gewünscht.

Die Forderung nach Manipulationssicherheit ist im Grunde genommen, dieselbe wie die Forderung nach Datenintegrität, einer der drei Säulen der Informationssicherheit, nach dem Modell der CIA-Triade [15]. In vielen wissenschaftlichen Quellen wird davon ausgegangen, dass DLT grundsätzlich sicher sind. Begründet wird dies mit den genutzten kryptographischen Verfahren und den verteilten Konsens. Anhand von Smart Contracts wurde bereits gezeigt, dass Anwendungen auf Grundlage von DLT nicht zwangsläufig sicher sind. Daher ist es wichtig an dieser Stelle zu prüfen, ob die oft getätigte Aussage „Blockchains sind sicher“ wirklich zutrifft und somit auch ihre Eignung Daten manipulationssicher zu verarbeiten.

Sicherheitsimplikationen durch DLT	Anzahl	Quellen
Manipulierbarkeit von Daten verringern	12	[21]; [26]; [27]; [31]; [32]; [33]; [35]; [36]; [40]; [43], [44]; [47]; [51];
Produktsicherheit für Verbraucher	6	[25]; [37]; [41]; [42]; [46]; [48]
Sicherheit in IoT Anwendungen (z.B. verhindern von DDOS-Attacken, Schutz von Updates)	4	[45]; [49]; [50]; [51]
Kein Single-Point of Failure	4	[30]; [32]; [44] [49];
Klärung von Haftungsfragen	2	[38]; [40]
Manuelle Eingaben gefährden das System	1	[25]

Tabelle 3 - Auswertung Literature Reviews Sicherheitsimplikationen durch DLT

Aufgrund des sich schnell entwickelnden Feldes an DLT gibt es bislang keine allgemeine Übersicht über die Sicherheit aller Systeme. Das liegt auch daran, dass zwar viele DLT ähnliche Konzepte nutzen, die sich jedoch in ihrer Implementierung stark unterscheiden können. Grundsätzlich gilt, dass zwar in vielen Publikationen behauptet wird, dass DLT sicher sind, jedoch kann es für kein System eine einhundertprozentige Sicherheit geben. Einschätzungen zur Sicherheit können daher nur für weitverbreitete Systeme wie Bitcoin oder Ethereum abgegeben werden. Implementationen von konsortialen oder Private Blockchains, können aufgrund der individuellen Anpassung nur im konkreten Anwendungsfall auf ihre Sicherheit hin untersucht werden.

Gefährdet waren Bitcoin und andere Blockchains bisher dort, wo Berührungspunkte zur Außenwelt bestehen. Gab es bis jetzt noch keinen erfolgreichen Angriff auf die Bitcoin-Blockchain, so wurden doch schon durch Hackerangriffe Bitcoins von Währungsbörsen oder anderen Applikationen gestohlen. Smart Contracts können, wie bereits angesprochen, ein weiterer Schwachpunkt sein. So wurden schon mehrmals durch falsch konfigurierte Smart Contracts auf Ethereum Angriffe möglich, die schwerwiegende finanzielle Schäden angerichtet haben [22]. Die Blockchains der beiden größten Netzwerke Bitcoin und Ethereum waren jedoch bis jetzt noch nicht betroffen. Somit ist bei der Betrachtung der Sicherheit zwischen der Technologieebene und der Anwendungsebene zu unterscheiden.

Trotzdem gibt es theoretische Angriffsmöglichkeiten auf die Blockchain an sich. Die bekannteste ist die sogenannte 51%-Attacke. Der Konsens wird verteilt getroffen, das heißt, dass immer ein zufälliger Knoten, anhand einer bestimmten Ressource, ausgewählt wird, der den nächsten Block propagieren darf. Erreicht eine Entität im Netzwerk mehr als die Hälfte der Ressourcen zu kontrollieren, bei einem PoW-Verfahren ist dies die Hashrate, so kann diese erfolgreich Double-Spends ausführen oder Transaktionen modifizieren [23]. Wie schwer es ist in einem Netzwerk 51% der Ressourcen zu sammeln ist von dem Aufbau und der Nutzerzahl abhängig. Dass eine einzelne Person 51% der Hashrate im Bitcoin-Netzwerk kontrolliert ist sehr unwahrscheinlich, da dies mit hohen Kosten verbunden wäre. Mining Pools können jedoch sehr nahe an diese Grenze stoßen, was ein Risiko darstellt. Daneben existieren andere mögliche Attacken, die an dieser Stelle nicht erörtert werden sollen, LI ET AL. (2017) geben dafür eine gute Übersicht. Das zeigt, dass Angriffe auf Blockchains möglich sind, verglichen mit zentralen Datenbanken verfügen sie jedoch über weitaus stärkere inhärente Schutzmechanismen, zumindest auf der Technologieebene [23].

Grundsätzlich eignen sich also DLT, um manipulationssicher Daten zu verarbeiten. Somit können DLT einen Beitrag zu Datenintegrität leisten und die Informationssicherheit stärken. Wenn von Datenintegrität die Rede ist, bezieht sich dies nicht nur auf den Schutz vor unerlaubter Veränderung der Daten von außen. Auch eine zentrale Instanz, die eine Datenbank verwaltet kann Einträge manipulieren, um daraus Vorteile zu ziehen. So könnte ein Logistikdienstleister die Datenbankeinträge über die Kühlung eines Produktes so manipulieren, dass ein Ausfall der Kühlung nicht mehr in den Einträgen auftaucht, um so Schadensersatzforderungen aus dem Weg zu gehen. Ist das System jedoch dezentral reicht es nicht aus, wenn eine Partei einen Manipulationsversuch startet, somit ist das System als Ganzes sicherer vor Manipulation.

Dadurch kann die Glaubhaftigkeit und Reputation von Informationen gesteigert werden, welche nach WANG UND STRONG (1996) Eigenschaften der Datenqualität darstellen [24]. Wie bereits geschildert korreliert die Datenqualität in vielen Untersuchungen mit der Performance der Supply Chain. Wodurch die Einführung von DLT einen positiven Beitrag zur Verbesserung der Leistung der ganzen Supply Chain leisten kann. Zu beachten gilt jedoch, dass andere Faktoren der Datenqualität nicht von der Blockchain beeinflusst werden. Ungenaue Eingaben, die auf menschliche Fehler zurückzuführen sind, können die Vorteile der Technologie wieder ausgleichen, da den Daten dadurch wieder nicht vertraut werden kann. Eine Nutzung der Technologie ist also nur ohne manuelle Dateneingabe sinnvoll [25].

Neben einer höheren Datenintegrität schaffen DLT mehr Sicherheit dadurch, dass sie keinen Single-Point-of-Failure aufweisen. Das heißt, dass wenn eine zentrale Datenbank angegriffen wird und dadurch nicht verfügbar ist, können die darin enthaltenen Daten nicht genutzt werden, was zu negativen wirtschaftlichen Konsequenzen führen kann. Fällt jedoch ein Knoten eines dezentralen Netzwerkes aus, können die Daten immer noch von den anderen Knoten abgerufen werden.

Ein letzter wichtiger Punkt, wie DLT Sicherheit verbessern kann bezieht sich indirekt auf die Akteure der Supply Chain. DLT kann es ermöglichen Verbrauchern mehr Produktsicherheit zu geben. Das bezieht sich vor allem auf Produkte wie Medikamente oder Nahrungsmittel. Wird ein Problem offenkundig z.B. eine Kontamination eines Nahrungsmittels, so kann durch die erhöhte Transparenz nachvollzogen werden, wo das Problem auftrat und Kunden können feststellen ob sie betroffen sind. Somit können Unternehmen schneller reagieren und geeignete Maßnahmen treffen das Problem zu beseitigen, was die Produktsicherheit erhöht.

10. Zusammenfassung

DLT scheinen eine Gruppe an Technologien zu sein, die Vorteile für SCM und Logistik bergen. Sie sind durch eine geringe Reife und Verbreitung gekennzeichnet, die sich zum einen an den Umsetzungsgraden von relevanten Projekten, zeigen. Zum anderen ist die Anzahl an wissenschaftlichen Veröffentlichungen, speziell im Spannungsbereich zwischen SCM und DLT, sehr gering. In der Auswertung der Literatur zum Thema wurde deutlich, dass teilweise unterschiedliche Auffassungen über die Definitionen und Eigenschaften von DLT bestehen. Daher sollten zukünftige Forschungsarbeiten weiter an einer Standardisierung der Definitionen arbeiten. Dies ist gerade nötig, da mittlerweile unter den Begriff DLT eine Vielzahl verschiedener Ausprägungen zusammengefasst werden. Außerdem finden sich in der Literatur keine Aussagen über die Quantifizierung der Vorteile, die DLT schaffen sollen. Auch hier sollte in der Zukunft ein Forschungsschwerpunkt liegen.

In der Untersuchung haben sich vier Bereiche herausgestellt, in denen sich Vorteile durch DLT erreichen lassen. Ein Bereich, der ganz klar mit der Herkunft von DLT als Zahlungssystem zusammenhängt, ist die Supply Chain Finance. Hier können DLT dazu beitragen, Prozesse zu automatisieren und zu digitalisieren. Dies ist dadurch möglich, dass es mit der Technologie erstmals möglich ist genuine digitale Originale zu schaffen. Dadurch wird eine stärkere Integration von Waren- und Zahlungsflüssen möglich.

Weitere Bereiche sind das Risikomanagement, SCV und die Integration von IoT-Netzwerken. Dabei dient der letztere Bereich vor allem als Basis für die vorher genannten. Das Internet-of-Things soll für die umfassende Abbildung der realen Welt im Digitalen sorgen, jedoch sind diese Anwendungen mit zahlreichen Sicherheitsproblemen behaftet. DLT wird als eine Art Kontrollebene gesehen, die Sicherheitsprobleme solcher Anwendungen mildern kann, was zu einer weiteren Verbreitung in der Industrie führen könnte. Zudem können DLT eine finanzielle Transaktionsebene zwischen einzelnen Geräten und Maschinen schaffen, womit neue Geschäftsmodelle ermöglicht werden.

Die Bereiche Risikomanagement und SCV profitieren von einer soliden Datenbasis aus IoT-Netzwerken, da sich dadurch ein schnelleres Reaktionsvermögen auf Ereignisse in der Supply Chain ergibt. Die Schaffung von Transparenz über Prozesse, Bestände, Nachfragen und Ereignisse trägt zu einer höheren Supply Chain Performance bei. Diese ist jedoch von der Qualität der Daten abhängig, wichtige Metriken sind hier die Glaubhaftigkeit, Reputation und Zugänglichkeit von Daten. DLT können diese Kategorien stärken, da sie es ermöglichen in einem Umfeld von Akteuren, die sich nicht vertrauen, Vertrauen zu schaffen. Dies ist durch die Dezentralität und der kryptographischen Absicherung der Anwendung der Fall. Es ist also für einen einzelnen Akteur nicht möglich Daten nachträglich zu manipulieren, die Datenintegrität und somit die Datensicherheit werden gestärkt. Dies vergrößert das Vertrauen in den Datenbestand, womit es für Unternehmungen einfacherer ist auf Basis der Daten Entscheidungen zu treffen. Des Weiteren wird durch die Dezentralität eine höhere Zugänglichkeit zu den Daten gewährt, da der Ausfall eines Knotens für das Gesamtsystem verkraftbar ist, weil der Datenzugriff über die anderen Knoten weiterhin möglich ist.

Literaturverzeichnis

[1] Bundesvereinigung Logistik (BVL) (2017): Logistikumsatz und Beschäftigung. Online verfügbar unter https://www.bvl.de/service/zahlen-daten-fakten/umsatz-und-beschaeftigung, zuletzt geprüft am 31.08.2020.

[2] Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2019): Die Lage der IT-Sicherheit in Deutschland 2019. Bonn. Online verfügbar unter https://bit.ly/3lGBwer.

[3] J. Sürmeli, U. Der, S. Jähnichen, A. Vogelsang (2017): Ein Rahmenwerk zur Protokollierung von Transaktionen in Distributed Ledgers. In: Informatik-Spektrum 40 (6), S. 595–601.

[4] V. Brühl (2017): Bitcoins, Blockchain und Distributed Ledgers. In: Wirtschaftsdienst 97 (2), S. 135–142.

[5] M. Kaulartz, J. Heckmann (2016): Smart Contracts – Anwendungen der Block-chain-Technologie. In: Computer und Recht 32 (9).

[6] V. Morabito (2017): Business Innovation Through Blockchain. Cham: Springer International Publishing

[7] M. Bartoletti, L. Pompianu (2017): An Empirical Analysis of Smart Contracts. Platforms, Applications, and Design Patterns. In: Michael Brenner, Kurt Rohloff, Joseph Bon-neau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague et al. (Hg.): Financial Cryptography and Data Security. Cham: Springer International Publishing, S. 494–509.

[8] J. Ream, Y. Chu, D. Schatsky (2016): Upgrading blockchains: Smart contract use cases in industry. Hg. v. Deloitte University Press. Online verfügbar unter https://bit.ly/32F5A17.

[9] C. Jentzsch (2016): Decentralized Autonomous Organization To Automate Govern-ance. Online verfügbar unter https://bit.ly/2QG79X6, zuletzt geprüft am 20.06.2020.

[10] M. Biederbeck (2016): Der DAO-Hack. Ein Blockchain-Krimi aus Sachsen. Online verfügbar unter

https://bit.ly/34PORuS, zuletzt geprüft am 22.06.2020.

[11] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi (2016): Step by Step Towards Creating a Safe Smart Contract. Lessons and Insights from a Crypto-currency Lab. In: J. Clark, S. Meiklejohn, P. Y.A. Ryan, D. Wallach, M. Brenner und K. Rohloff (Hg.): Financial Cryptography and Data Security. FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers. Berlin: Springer. (Lecture Notes in Computer Science), S. 79–94.

[12] L. Luu, D. Chu, H. Olickel, P. Saxena, A. Hobor (2016): Making Smart Contracts Smarter. In: E. Weippl und S. Katzenbeisser (Hg.): CCS '16. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, S. 254–269.

[13] I. Nikolic, A. Kolluri, I. Sergey, P. Saxena, A. Hobor, (2018): Finding The Greedy, Prodigal, and Suicidal Contracts at Scale.

[14] W. Blocher (2018): C2B statt B2C? Auswirkungen von Blockchain, Smart Contracts & Co. auf die Rolle des Verbrauchers. In: P. Kenning und J. Lamla (Hg.): Entgrenzungen des Konsums. Dokumentation der Jahreskonferenz des Netzwerks Verbraucherforschung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 87–108.

[15] Y. Cherdantseva, J. Hilton (2013): A Reference Model of Information Assurance & Security. In: 2013 International Conference on Availability, Reliability and Security. ARES 2013. Regensburg, 02.-06.09.2013. The Institute of Electrical and Electronics Engineers, Inc. Piscataway: IEEE, S. 546–555.

[16] X. Xu, C. Pautasso, L. Zhu, V. Gramoli,A. Ponomarev, A. Tran, S. Chen (2016): The Blockchain as a Software Connector. In: H. Muccini und K. E. Harper (Hg.): WICSA 2016. 2016 13th Working IEEE/IFIP Conference on Software Architecture: proceedings. Venedig. Piscataway: IEEE, S. 182–191.

[17] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi (2016): Town Crier. An Authenticated Data Feed for Smart Contracts. In: E. Weippl und S. Katzenbeisser (Hg.): CCS '16. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, S. 270–282.

[18] S. Ellis, A. Juels, S. Nazarov (2017): ChainLink. A Decentralized Oracle Network. Online verfügbar unter https://link.smartcontract.com/whitepaper.

[19] C. F. Durach, J. Kembro, A. Wieland (2017): A New Paradigm for Systematic Literature Reviews in Supply Chain Management. In: J Supply Chain Manag 53 (4), S. 67–85.

[20] D. Denyer, D. Tranfield (2009): Producing a Systematic Review. In: D. A. Buchanan und A. Bryman (Hg.): The Sage handbook of organizational research methods. Los Angeles: Sage, S. 671–689.

[21] R. Stahlbock, L. Heilig, S. Voß (2018): Blockchain in der maritimen Logistik. In: HMD Praxis der Wirtschaftsinformatik, S. 1–19.

[22] M. Orcutt (2018): How secure is blockchain really? It turns out "secure" is a funny word to pin down. MIT Technology Review. Online verfügbar unter https://bit.ly/3gGej8p.

[23] X. Li, O. Jiang, T. Chen, X. Luo, Q. Wen (2017): A survey on the security of blockchain systems. In: Future Generation Computer Systems.

[24] R. Wang, D. M. Strong (1996): Beyond accuracy. What data quality means to data consumers. In: Journal of Management Information Systems 12 (4), S. 5–33.

[25] T. K. Agrawal, A. Sharma, V. Kumar (2018): Blockchain-Based Secured Traceability System for Textile and Clothing Supply Chain. In: S. Thomassey und X. Zeng (Hg.): Artificial Intelligence for Fashion Industry in the Big Data Era. Singapore: Springer, S. 197–208.

[26] H. R. Hasan, K. Salah (2018): Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters. In: IEEE Access 6, S. 46781–46793.

[27] T. Bocek, B. B. Rodrigues, T. Strasser, B. Stiller, (2017): Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In: P. Chemouil (Hg.): Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network Management. Lissabon. Piscataway: IEEE, S. 772–777.

[28] A. Bahga V. K. Madisetti (2016): Blockchain Platform for Industrial Internet of Things. In: Journal of Software Engineering and Applications 9, S. 533.

[29] M. Kupferberg, P. Sandner, M. Felder (2018): Blockchain-basierte Abrechnung der IoT-registrierten Stationshalte: ein Proof-of-Concept auf Basis von Ethereum. Frankfurt am Main.

[30] K. Korpela, J. Hallikas, T. Dahlberg: Digital Supply Chain Transformation to-ward Blockchain Integration. In: Hawaii International Conference on System Sciences 2017 (HICSS-50). Hawaii, January 4-7, 2017. Hawaii International Conference on System Sciences; HICSS, S. 4182–4191.

[31] E. Hofmann, U. M. Strewe, N. Bosia (2018): Supply Chain Finance and Blockchain Technology. Cham: Springer International Publishing.

[32] Y. Omran, M. Henke, R. Heines, E. Hofmann, (2017): Blockchain-driven supply chain finance. Towards a conceptual framework from a buyer perspective. In: IPSERA 2017. Budapest, S. 1–15.

[33] M. Witthaut, H. Deeken, P. Sprenger, P. Gadzhanov, M. David (2017): Smart Objects and Smart Finance for Supply Chain Management. In: Logistics Jounal: referierte Veröffentlichungen 2017 (10).

[34] B. Nicoletti (2018): Agile Procurement. Volume II: Designing and Implementing a Digital Transformation. Cham: Springer International Publishing.

[35] S. Tönnissen, F. Teuteberg (2018): Using Blockchain Technology for Business Processes in Purchasing. Concept and Case Study-Based Evidence. In: W. Abramowicz und A. Paschke (Hg.): Business Information Systems. Cham: Springer International Publishing (320).

[36] S. C. Eickemeyer, T. Halaszovich, C. Lattemann, (2018): Blockchain Technologien für die Sicherung von Material-, Informations- und Geldflüssen in der Logistik – Erfolgsfaktoren für die chinesische „Belt-Road“ Initiative. In: HMD Praxis der Wirtschaftsinformatik, S. 1–14.

[37] Y. Cui, H. Idota (2018): Improving Supply Chain Resilience with Establishing A Decentralized Information Sharing Mechanism. In: Proceedings of the 5th Multidisciplinary International Social Networks Conference - MISNC '18. Saint-Etienne, 16-18. Juli 2018. New York: ACM Press, S. 1–7.

[38] A. Imeri, C. Feltus, D. Khadraoui, N. Agoulmine, D. Nicolas (2018): Solving the trust issues in the process of transportation of dangerous goods by using blockchain technology. In: P. Reinecke, P. Burnap, N. Moradpoor, A. Elçi, G. Theodorakopoulos, O. Rana und K. Karabina (Hg.): Proceedings of the 11th International Conference on Security of Information and Networks - SIN '18. Cardiff, 10/9/2018 - 12/9/2018. New York: ACM Press, S. 1–2.

[39] B. Alangot, K. Achuthan (2018): Trace and Track: Enhanced Pharma Supply Chain Infrastructure to Prevent Fraud. In: N. Kumar und A. Thakre (Hg.): Ubiquitous Communications and Network Computing. First International Conference, UBICNET 2017, Bangalore, India, August 3-5, 2017, Proceedings, S. 189–195

[40] B. Yahsi (2017): Financial Supply Chain Management. Erfolgsfaktoren der Gestaltung von Finanznetzwerken. Dissertation, Darmstadt, Technische Universität Darmstadt, 2017.

[41] Q. Lu, X. Xu (2017): Adaptable Blockchain-Based Systems. A Case Study for Product Traceability. In: IEEE Softw. 34 (6), S. 21–27.

[42] V. A. J. Boehm J. Kim, J. W. Hong (2018): Holistic Tracking of Products on the Blockchain Using NFC and Verified Users. In: B. Kang und T. Kim (Hg.): Information security applications. 18th international conference, WISA 2017, Jeju Island, Korea, August 24-26, 2017 : revised selected papers. Cham: Springer (Lecture Notes in Computer Science, 10763), S. 184–195.

[43] F. Tian (2017): A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In: J. Tang, J. Chen und X. Cai (Hg.): The 14th International Conference on Services Systems and Services Management (ICSSSM2017). June 16-18, 2017, Dalian, China : proceedings. Piscataway: IEEE, S. 1–6.

[44] A. Reyna, C. Martín, J. Chen; E. Soler, M. Díaz, (2018): On blockchain and its integration with IoT. Challenges and opportunities. In: Future Generation Computer Systems 88, S. 173–190.

[45] K. Christidis, M. Devetsikiotis (2016): Blockchains and Smart Contracts for the Internet of Things. In: IEEE Access 4, S. 2292–2303.

[46] K. Toyoda. T. Mathiopoulos, I. Sasase, T. Ohtsuki (2017): A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. In: IEEE Access 5, S. 17465–17477.

[47] Y. Yang, Y. Yang, J. Chen, M. Liu (2018): Application of Blockchain in Internet of Things. In: X. Sun, Z. Pan und E. Bertino (Hg.): Cloud Computing and Security. 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part II. Cham: Springer International Publishing (11064), S. 73–82.

[48] H. L. à Nijeholt,J. Oudejans, Z. Erkin (2017): DecReg. A Framework for Preventing Double-Financing using Blockchain Technology. In: S. Lokam, S. Ruj und K. Sakurai (Hg.): Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17. Abu Dhabi. New York: ACM Press, S. 29–34.

[49] N. Kshetri (2017): Can Blockchain Strengthen the Internet of Things? In: IT Prof. 19 (4), S. 68–72.

[50] D. Minoli, B. Occhiogrosso (2018): Blockchain mechanisms for IoT security. In: Internet of Things 1-2, S. 1–13.

[51] M. A. Khan, K. Salah (2018): IoT security. Review, blockchain solutions, and open challenges. In: Future Generation Computer Systems 82, S. 395–411.