

Die Blockchain Technologie (BCT) zur Verbesserung von Transaktionsprozessen in der Logistik

Blockchain technology (BCT) to improve transaction processes in logistics

Simeon Eberlein und Herwig Winkler

Lehrstuhl für Produktionswirtschaft
Brandenburgische Technische Universität Cottbus-Senftenberg

Blockchain-Technologie ist die Zukunft im Bereich sicherer Datenspeicherung und -nachverfolgung. Dabei wird diese Technologie schon lange nicht mehr nur bei Kryptowährungen eingesetzt. Viele Unternehmen arbeiten und entwickeln Lösungen, um mit der Blockchain-Technologie Prozessverbesserung in der Industrie zu realisieren. Vor allem Transaktionsprozesse in der Logistik können durch den Einsatz dieser Technologie optimiert werden. Demnach ist das Ziel dieses Artikels die Grundzüge der Blockchain Technologie darzulegen und aufzuzeigen, wo die Blockchain bereits genutzt wird und wie dadurch Logistikprozesse verbessert werden. Der Fokus dieses Beitrags liegt auf Blockchain-Anwendungen, die sich bereits in der Industrie etabliert haben. Es wird analysiert, wie diese Systeme aufgebaut sind, wie sie in der Praxis eingesetzt werden und welchen Verbesserungen mit ihnen zu realisieren sind.

[Keywords: Blockchain, Logistic, Smart Contracts, TradeLens, IBM Food Trust]

Blockchain technology is the future of secure data storage and tracking. This technology has long been used for more than just cryptocurrencies. Many companies are working on and developing solutions to improve processes in industry with blockchain technology. Above all, transaction processes in logistics can be optimised through the use of this technology. Accordingly, the aim of this article is to elaborate where blockchain is already being used and how it can improve logistics processes. We will first give a brief overview of the most important basics of blockchain. The focus of this article is then on blockchain applications that have already established themselves in industry. We will analyse how these systems are structured, how they are used in practice and which optimisations can be realised with them.

[Keywords: Blockchain, Logistic, Smart Contracts, TradeLens, IBM Food Trust]

1 EINFÜHRUNG IN DIE BLOCKCHAIN-TECHNOLOGIE

Die Blockchain-Technologie wird oft mit Kryptowährungen assoziiert. Es ist jedoch anzumerken, dass Kryptowährungen nur ein Randprodukt der Blockchain-Technologie sind. Blockchain ähnliche Modelle gab es wesentlich früher als Bitcoin, Ethereum etc. [PSSK19]. Allerdings brachten erst Kryptowährungen die Blockchain-Technologie in das öffentliche Interesse. Die Grundlage dafür war das Dokument „Bitcoin: A Peer-to-Peer Electronic Cash System“, welches im Jahr 2008 erschien und von dem Synonym Satoshi Nakamoto verfasst wurde. Von da an begann der Triumphzug der Kryptowährungen aber auch der Blockchain-Technologie.

Die Blockchain-Technologie kann als eine Verkettung von Daten definiert werden, die eine dezentrale Dateninfrastruktur mit unverwechselbaren architektonischen Eigenschaften gegenüber anderen Technologien besitzt. Eine Blockchain besteht aus einem Peer-to-Peer (P2P) Netzwerk, einer kryptografischen Verschlüsselung und einem Konsensmechanismus [WHB19]. Das P2P Netzwerk ermöglicht eine dezentrale Struktur, die eine bessere Zugänglichkeit auf Datensätze für Teilnehmer des Netzwerkes ermöglichen. Die kryptografische Verschlüsselung sorgt für eine genaue Nachverfolgung und für die Unveränderlichkeit der Daten. Der Konsensmechanismus kodiert die Transaktionen mithilfe der kryptografischen Verschlüsselung in Blöcke und ermöglicht so ein kontinuierliches Wachstum der Blockchain [NK17].

1.1 BLOCKCHAIN ARCHITEKTUR

Wird von einem Blockchain-basierten System gesprochen, so handelt sich es in den meisten Fällen um ein Peer-to-Peer Netzwerk. Die Peers sind all die Personen, die an dem Netzwerk teilnehmen. Um Teil des Systems zu werden müssen die Nutzer eine entsprechende App herunterladen. Diese heruntergeladene App stellt nun ein Knoten im Netzwerk dar. Allen Knoten sind in einem Peer-to-Peer Netzwerk gleichberechtigt und miteinander verbunden. Sie können untereinander Dienste anbieten oder in Anspruch nehmen. Die Kommunikation in einem P2P- Netzwerk

findet über eine unverschlüsselte Internetverbindung statt, da es keine Authentifizierungsmechanismen gibt und die Nutzer keine zentrale Anlaufstelle haben [MG20].

Auch in einem Blockchain-basierenden Netzwerk sind alle miteinander verbunden und haben die gleichen Rechte. Jedoch gibt es in diesem dezentralen Netzwerk meist drei unterschiedliche Arten von Teilnehmern:

- **User (Light-Nodes):** Sie bilden die größte Gruppe in einem dezentralen Netzwerk und wollen hauptsächlich nur Zahlungen tätigen und empfangen. Andere Handlungen werden von ihnen meist nicht getätigt. Viele dieser User haben nicht die Kapazität die ganze Blockchain bei sich zu sichern. Aus diesem Grund speichern sie nur einen kleinen Teil der gesamten Blockchain bei sich ab. Möchte ein User eine Zahlung tätigen, so schickt er seine Anliegen an einen Node oder Miner. Diese leiten die Intention weiter, um mit dem gesamten Netzwerk einen Konsens zu bilden. Für diesen Aufwand zahlt der User eine Mining-Gebühr [MG20].
- **Full-Nodes oder Nodes:** Sie speichern die gesamte Blockchain bei sich ab, damit sichergestellt werden kann, dass das Netzwerk dezentral bleibt. Des Weiteren überprüfen sie Informationen von Usern oder anderen Nodes und leiten sie im Anschluss an die Miner weiter [MG20].
- **Miner:** Diese spezielle Gruppe erstellt die Blöcke einer Blockchain und erzeugt den Konsens im Netzwerk. Dafür überprüfen und verifizieren sie Transaktionen, die Teilnehmer durchführen möchten.

Es kann vorkommen, dass ein Teilnehmer in allen drei Gruppen vertreten ist. Dies ist relativ selten, da in den meisten blockchain-basierten Netzwerken die Rollen voneinander getrennt sind. In der Regel wollen die meisten Nutzer nur Kryptowährungen handeln und sich nicht mit der Sicherheit dahinter beschäftigen. Aus diesem Grund gibt es die Aufteilung in drei Gruppen.

1.2 PUBLIC-KEY-KRYPTOGRAPHIE UND HASHFUNKTION

Die Public-Key-Kryptografie funktioniert ähnlich wie ein Briefkasten. Der Briefkasten ist für jeden sichtbar, der den Standort kennt. Im Grunde heißt das, dass der Standort des Briefkastens öffentlich bekannt ist. Jeder, der die Adresse kennt, kann zum Briefkasten gehen und einen Brief einwerfen. Den Briefkasten kann aber nur der Besitzer mit dem passenden Schlüssel öffnen und die Nachrichten lesen. Das Prinzip der Public-Key-Kryptografie ist ähnlich, wie das Briefkastenprinzip. Bei dieser Verschlüsselungsart haben zwei Parteien jeweils einen Private Key und einen Public Key. Um die Schlüssel zu generieren, wird in der

Regel der RSA-Algorithmus genutzt. Dieser Algorithmus schafft es zwei Schlüssel (Public- und Private Key) zu erstellen, die mathematisch miteinander verknüpft sind. Der Public Key hat die Aufgabe die Daten so zu verschlüsseln, dass sie nur vom entsprechenden Private Key entschlüsselt werden können. Die beiden Schlüssel bauen aufeinander auf, können aber nicht voneinander abgeleitet werden. Das heißt, wenn der Public Key von einer Partei bekannt ist, ist es Dritten so gut wie unmöglich den Private Key herauszufinden. In der Metapher vom Anfang ist die Adresse des Briefkastens der Public Key und der Schlüssel des Besitzers der Private Key. Bei einer Transaktion mit der Public-Key-Kryptografie tauschen die Parteien untereinander ihre Public Keys aus. Nun kann Partei A Partei B ein Transaktionsobjekt, z.B. Informationen, digitales Geld, Bilder etc. schicken. Dazu wird der Public Key von Partei B genutzt, um die Nachricht von Partei A zu verschlüsseln. Anschließend wird das Transaktionsobjekt von Partei A an Partei B geschickt. Partei B kann mit seinem Private Key, das Transaktionsobjekt, entsperren und verwenden (siehe Abbildung 1) [MG20]. Der Vorteil bei dieser Verschlüsselungsart ist, dass nur Partei B mit seinem Private Key das Transaktionsobjekt empfangen und nutzen kann. Die Voraussetzung dafür ist, dass Partei B seinen Private Key nicht teilt oder weitergibt.

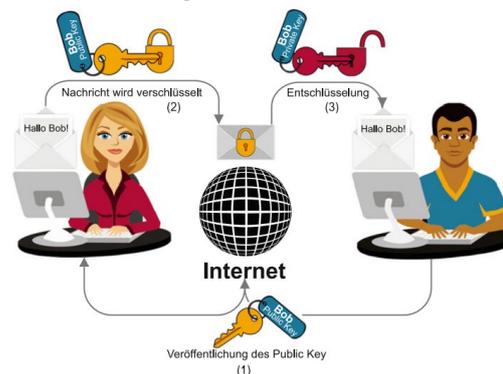


Abbildung 1. Public-Key-Kryptografie [MG20]

Die Hashfunktion ist ebenso wie die Public Key Kryptografie ein Algorithmus, der zur Verschlüsselung dient. Sie wandelt einen Datensatz von unterschiedlicher Länge in eine hexadezimale Zeichenkette mit einer festen Länge (Hashwert) um. Beim Secure Hash Algorithm (SHA-256), der bei Bitcoin zum Einsatz kommt, ist diese Länge 256 Zeichen/Bits lang. Dabei setzt sich der Hashwert aus Zahlen- und Buchstabenkombinationen zusammen. Durch die Hashfunktionen können Nachrichten unverwechselbar und einwandfrei identifiziert werden. Aus diesem Grund ist die Hashfunktion auch als Fingerabdruck bekannt. In der Praxis füttert ein Nutzer die Hashfunktion mit einer Kryptowährung oder einer Nachricht, wie zum Beispiel „DHL Paket ist da“. Diese Nachricht wird nun in einen 256 langen Hashwert (z.B. A45DFget33...) umgewandelt und anschließend mit dem Public Key signiert und abgeschickt. Der Empfänger der Datei kann nun mit seinem Private Key den Hashwert entschlüsseln und den Text „DHL Paket ist da“ lesen. Möchten nun ein Hacker den Hashwert knacken,

in dem er den erstellten Hashwert erneut mit der Hashfunktion füttert, in der Hoffnung, dass „DHL Paket ist da“ herauskommt, so würden aus „A45DFget33...“ ein komplett neuer Hashwert (z.B. rrTDG45w12...) generiert werden [MG20].

1.3 KONSENSMECHANISMUS

Ein Konsensmechanismus ist ein komplexes Verfahren durch den ein Konsens in einer Blockchain entsteht. Dieser Prozess startet, indem ein Teilnehmer der Blockchain eine Transaktion mit seinem Private Key unterschreibt. Im Grunde genommen bedeutet dies, dass der User eine Public Adresse angibt, an der das Geld gesendet werden soll. Anschließend wird diese Transaktion an einen Miner oder Node (Node kann auch als Miner auftreten) weitergeleitet, welcher die Transaktion wiederum an weitere Miner oder Nodes leitet. Der Vorgang endet, wenn alle Teilnehmer im Netzwerk diese Information bekommen haben.

Erhält ein Miner eine Transaktion so überprüft er, ob sie auch korrekt ist. Das heißt es wird kontrolliert, ob richtig mit dem Private Key unterschrieben wurde, an welche Public Adresse die Transaktion gesendet wird und ob es ausreichend Geld/Coins zu senden gibt. Für den Aufwand die Transaktionen zu überprüfen, erhält der Miner eine Belohnung (Kryptowährungen und/oder Gebühren). Das Prüfen von Transaktionen macht der Miner mit etlichen Transaktionen. Damit der Miner nicht böswillig agiert und die Leute bestiehlt wurden sogenannte Konsensmechanismen für die Blockchain-Technologie entworfen. Die Intention hinter diesen Mechanismen ist, dass die Mehrheit der ehrlichen Nutzer über die Kontrolle der Blockchain verfügen. Möchte ein Miner nun Kontrolle haben, um Transaktion zu überprüfen, so muss er sich mittels dem Proof-of-Work Algorithmus als würdig erweisen. Der Proof-of-Work Algorithmus ist der älteste und am meisten verwendete Konsens-Algorithmus. Er ist Bestandteil der Bitcoin-Blockchain. Der Grund für seine Beliebtheit liegt an der hohen Widerstandsfähigkeit gegenüber den anderen Algorithmen. Bei Proof-of-Work muss der Miner beweisen, dass er Arbeit geleistet hat. Schafft es ein Miner diese Arbeit als erster zu erledigen, bekommt er die Mining-Belohnung und darf den Block erstellen. Die Arbeit, die ein Miner zu erledigen hat, ist das sog. Reverse Engineering (Rückrechnen) eines schwierigen kryptografischen Algorithmus. Der kryptografische Algorithmus kann nur durch wiederholtes Ausprobieren verschiedener Hashwerte gelöst werden. Dazu muss der Miner fähig sein 15 Mio. Hasches in einer Sekunde auszuprobieren [MG20]. Das Reverse Engineering ist wie ein Puzzle aus verschiedenen Transaktionen zusammengesetzt. Schafft es ein Miner das Puzzle zu lösen und den Block zu erstellen schickt er sein Puzzle an alle Nodes und Miner [FHM20]. Anschließend überprüfen die Teilnehmer des Netzwerkes, an denen das Puzzle geschickt wurde, auf seine Richtigkeit. Wird der Block von

51% als korrekt angesehen, so kann er an die Blockchain angehängt werden.

Neben dem Proof-of-Work Algorithmus gibt es noch den Proof-of-Stake. Bei diesem Konsensmechanismus wird auf die Wichtigkeit des Geldes gesetzt. Der Miner, der mehr Geld im System besitzt, erhält eine größere Wahrscheinlichkeit mittels Zufallsprinzip für das Mining ausgewählt zu werden. Möchte ein Miner den Auftrag bekommen, so muss er viel Geld investieren, um seine Wahrscheinlichkeit zu erhöhen. Proof-of-Stake hat viele Kritiker, da befürchtet wird, dass viele Reiche die gesamte Konsens-Macht haben und armen Miner die Möglichkeit genommen wird, Mining zu betreiben. Es gibt ein paar Blockchain-Anwendungen, z.B. Cardano, bei denen der Proof-of-Stake Algorithmus funktioniert [Car20].

Auch der Proof-of-Importance Algorithmus ist nicht unumstritten, da der Miner nachweisen muss, dass er wichtig ist. Ob er wichtig ist, hängt von der Blockchain-Anwendung ab. Aber in der Regel wird dies mittels eines Berechnungsmodelles ermittelt. Die Faktoren, die für die Berechnung miteinfließen sind folgende: wie lange er schon im System ist und wie viele andere Nutzer sich mit ihm vernetzen wollen. Der Vorteil den Proof-of-Importance mit sich bringt ist, dass jeder, unabhängig vom Reichtum, den Mining-Auftrag bekommen kann. Er muss nur an Bedeutung gewinnen. Auf der anderen Seite kann das System von betrügerischen Teilnehmern geschwächt werden, wenn sie sich mit Fake-Accounts untereinander vernetzen und für sich abstimmen. Proof-of-Importance ist noch ein relativ junger Algorithmus, der in Zukunft noch an Bedeutung gewinnen kann [Sch19].

1.4 SMART CONTRACTS

Zum ersten Mal fiel der Begriff Smart Contracts in einem Artikel von Nick Szabao im Jahr 1994. Die erste Intention von Smart Contracts unterscheidet sich nicht stark von den heutigen. Früher sollten Smart Contracts eine digitalisierte Vertragsbedingung sein, die ohne Einfluss von Dritten automatisch ausgeführt werden. Heutzutage sind Smart Contracts Programme, die auf einer Blockchain gespeichert sind und unter bestimmten Voraussetzungen automatisch ausgeführt werden. Da die Smart Contracts auf der Blockchain gespeichert sind, sind sie dezentral und unveränderlich. Diese beiden Eigenschaften machen Smart Contracts zu einem zuverlässigen und vertrauenswürdigen Instrument. Durch die Unveränderlichkeit der virtuellen Verträge kann niemand am Code des Vertrages etwas ändern. Aus diesem Grund muss vorher genau durchdacht werden, ob der Smart Contract die Dinge erfüllt, für die er programmiert wurde. Durch die Dezentralisierung wird sichergestellt, dass niemand den Vertrag zwingt, z.B. Geld freizugeben, bevor die vorher definierte Bedingung erfüllt wurde. Jeder Teilnehmer im Netzwerk validiert die Ausgabe des Vertrages, sodass keine Freigabe erteilt wird ohne, dass es anderen Personen im Netzwerk auffallen

würde [LSS20]. Smart Contracts sind vielseitig einsetzbar. Banken könnten sie nutzen, um Kredite zu vergeben oder automatische Zahlungen anzubieten. In der Versicherungsbranche können sie genutzt werden, um bestimmte Ansprüche zu bearbeiten oder bei Todesfällen automatisch Geld auszuzahlen. Postunternehmen könnten sie für die Zahlung bei Lieferung verwenden. Die bekannteste Anwendung für Smart Contracts sind die Kryptowährungen. Ethereum war die erste digitale Währung, die ihre Grundfunktionalitäten um Smart Contracts erweitert hat. Die Entwicklung eines Smart Contracts für Ethereum erfolgt beispielsweise über die Programmiersprache Solidity. Diese gibt dem Smart Contract seine Funktionen [LSS20].

Neben den ganzen Vorteilen von Smart Contracts sollte ein Aspekt nicht vernachlässigt werden; nämlich die Tokenisierung von digitalen Verträgen an kritischen Stellen. Ein Beispiel ist die Anwendung von Smart Contracts in der Versicherungsbranche. Möchte eine Versicherung beispielsweise eine Lebensversicherung als Smart Contract definieren, mit der Bedingung, dass bei Eintritt des Todesfalls das Geld an die Hinterbliebenen ausgeschüttet wird, könnten Personen diesen Smart Contract tokenisieren und darauf oder dagegen wetten, ob die betroffene Person im Jahr X stirbt. Das Gleiche tritt auch bei einer Brandschutzversicherungen oder einer Unfallversicherung ein. Der Grund dafür, dass solche Wetten möglich sind, liegt an der Dezentralisierung der Smart Contracts. Es gibt keine zentrale Institution, die solche Wetten unterbinden kann. Diese Fälle existieren aktuell noch nicht oder sind nur vereinzelt bekannt, könnten aber mit dem stetigen Fortschreiten der Smart Contracts in der Zukunft ein Problem werden [Hay18].

2 SYSTEMATISCHE LITERATURERECHERCH

Für die Literaturrecherche wurden die Datenbanken von „Web of Science“, „Science Direct“ und vom „Springer Link“ genutzt. Zu Beginn der Recherche wurde auf „Web of Science“ und Science Direct“ mit dem Algorithmus „TS=(blockchain AND process AND (production OR logistic*))“ gesucht. In „Web of Science“ ergaben sich 226 Publikationen und auf „Science Direct“ über 1000. Diese wurden jedoch durch eine Selektion der Themenbereiche auf 291 Ergebnisse eingeschränkt. Dabei wurden Werke aussortiert, die vor 2010 veröffentlicht oder nicht in Journalen mit Bezug zur Logistik oder Produktion, publiziert wurden. Zu den Publikationen aus den Online-Datenbanken kam noch die Literatur aus dem Springer Link (vier Publikationen) und aus der Eigenrecherche (zehn Publikationen) hinzu, so dass am Ende 531 Publikationen zur Verfügung standen. Aus der Gesamtsumme von 531 Werken konnten 43 aufgrund von Duplikaten ausgeschlossen werden. Von den verbleibenden 488 Veröffentlichungen mussten 403 aussortiert werden, da ihr Abstract oder Titel keinen Bezug zum Thema hatten. Die verbleibenden 85 Publikationen kamen in die detaillierte Analyse, so dass am

Ende 44 Publikationen für das Forschungsgebiet relevant waren. Die folgende Tabelle unterteilt die Literatur in die

Themenbezug	Anzahl	Prozentuale Verteilung
Gesamte Literatur	44	100,00%
Hohe Relevanz	14	31,81%
Niedrige Relevanz	10	22,72%
Bedingte Relevanz	9	20,45%
Keine Relevanz	11	25,00%

Tabelle 1. Die Relevanz der Publikationen zum Forschungsthema

Kategorien: Hohe Relevanz, Niedrige Relevanz, Bedingte Relevanz und Keine Relevanz

Von den 44 Publikationen konnten 14 Werke eine hohe Relevanz zum Thema aufweisen, zehn Werke hatten nur eine niedrige Relevanz zum Thema, neun Publikationen waren nur bedingt relevant für die Recherche und elf Werke hatten gar keinen Nutzen für die Ausarbeitung der Seminararbeit. Die detaillierte Auflistung der 14 Werke mit Autor, Titel, Journal und Kurzzusammenfassung ist am Ende dieser Publikation als Tabelle 3 zu finden.

In Tabelle 2 ist zu erkennen welche Arten von Dokumenten gefunden wurden. Der kleinste Teil in dieser Kategorie bilden die vier Bücher. Der größte Teil sind die Artikel mit einer Anzahl von 17 Werken, gefolgt von den Reviews mit 14 und den Papers mit 10 Publikationen.

Art der Publikationen	Anzahl	Prozentuale Verteilung
Bücher	4	9,09%
Artikel	17	38,63%
Reviews	13	29,54%
Papers	10	22,72%

Tabelle 2. Arten der Publikationen zum Forschungsthema

Des Weiteren wurde die Literatur in ihre Erscheinungsdaten unterteilt (siehe Abbildung 2). Sieben der 44 Publikationen erschienen im Jahr 2021. 16 Publikationen wurden 2020 veröffentlicht und im Jahr 2019 waren es zehn Werken. In den Jahren 2018 bis 2016 wurden



Abbildung 2. Publikationsjahre der Publikationen

zwischen vier und zwei Werken veröffentlicht. Die Jahre 2010 und 2008 hatten jeweils nur eine relevante Publikation.

Als letztes wurden die Schlüsselwörter der Publikationen ausgewertet. Zur Vereinfachung wurden nicht alle Wörter berücksichtigt, sondern nur die, die am häufigsten verwendet wurden. In der Wortwolke (siehe Abbildung 3) befinden sich Wörter mit unterschiedlicher Gewichtung, je größer das Wort desto häufiger wurde es angegeben. Blockchain war mit Abstand das am meisten genutzte Wort; gefolgt von Supply Chain Management, Smart Contracts und Kryptografie. Am seltensten wurde das Wort Sustainability und Internet of Things genutzt.



Abbildung 3. Wortwolke zu den Schlüsselwörtern der Publikationen

Aktuell konzentriert sich die Forschung darauf innovative Technologien wie Internet of Things, künstliche Intelligenz und die Blockchain-Technologie zusammenzubringen. Es sollen vor allem in Industriebereichen wie Supply Chain Management, Produktion und Logistik durch die erfolgreiche Kombination dieser Technologien Erfolgspotenziale realisiert werden.

3 BLOCKCHAINBASIERTE PLATTFORMEN ZUR UNTERSTÜTZUNG VON TRANSAKTIONSPROZESSEN IN DER LOGISTIK

3.1 TRADELENS

TradeLens ist eine Plattform für Spediteure, Häfen, Redereien und alle Unternehmen oder Ämter, die ein Teil der Supply Chain in der Containerlogistik sind. Aktuell gibt es ca. 65 eingebundene oder in Bearbeitung befindliche Netzwerkmitglieder, 18 Handelsdokumenttypen, die unterstützt werden und 1,5 Mio. täglich erfasste Versandereignisse. TradeLens wurde erstmals im März 2017 von den Gründern IBM und Maersk angekündigt und im August 2018 ging die Plattform zum ersten Mal online. Die Intention von IBM und Maersk ist es die in der Schifffahrtsindustrie herrschenden Probleme zu verbessern und zu eliminieren. Es werden Versanddaten auf verschiedenen Papieren oder digitalen Systemen gespeichert. Dies führt zu Verzögerungen, Inkonsistenz und blinden Flecken, welche wiederum zu schlechten Entscheidungen führen. Durch Zollabfertigungen, die ein hohes Maß an Sorgfalt

benötigen, um Fälschungen zu verhindern, entsteht oft Sendungsstau. Des Weiteren sind Unternehmen eingeschränkt Prognosen zu erstellen und verifizierte Informationen auszutauschen. Daraus resultieren oft operative Herausforderungen und ein schlechter Kundenservice. Wegen diesen Problemen versuchen IBM und Maersk mit TradeLens die verschiedenen Gruppen in der Supply Chain auf eine Plattform zu bringen und sie zur Zusammenarbeit und zum Austausch von Informationen zu bewegen [YT19].

3.1.1 AUFBAU VON TRADELENS

TradeLens baut auf den Säulen: Netzwerk, Plattform, Anwendungen und Services auf (siehe Abbildung 4). Jeder dieser drei Säulen hat unterschiedliche Funktionen und Bestandteile. Das Netzwerk besteht aus den Mitgliedern von TradeLens. Zu diesen Mitgliedern zählen Spediteure, Häfen und Zollämter. Diese Entitäten stellen sich gegenseitig Daten zu Verfügung und speichern selbst Daten auf der Plattform. Der Zugriff zur TradeLens Plattform ist mittels einer offenen **Application Programming Interface (API)** möglich. Auf dieser Plattform ist es den Beteiligten der Supply Chain gestattet untereinander in Verbindung zu treten und Informationen auszutauschen. Damit der Austausch sicher ist wird die TradeLens Plattform von Blockchain- und Cloud-Technologie unterstützt. Der letzte Aspekt sind die Anwendungen und Services. Sie ermöglichen Teilnehmern einheitliche und vorgefertigte Dokumente oder andere Anwendungen zu nutzen. Des Weiteren können die Nutzer auch neue Applikationen auf dieser Plattform programmieren [YT19].

Wie bereits erwähnt ist TradeLens eine Plattform, die eine Reihe von Diensten und Anwendungen anbietet. Sie sollen den Informationsaustausch zwischen den Beteiligten der Supply Chain erleichtern. All diese Dienste und Anwendungen sind auf der Blockchain gespeichert. Damit eine Blockchain-Anwendung wie TradeLens erfolgreich funktioniert, benötigt es ein großes Ökosystem an verschiedenen Nutzern. Für den Aufbau eines Ökosystems benötigt es sog. Trustanchors. Trustanchors sind die Schlüsselspieler in dem System. Sie ziehen die anderen Akteure nach [Grä21]. Im Beispiel von TradeLens sind die Trustanchors Seetransportunternehmen wie Maersk, Hamburg-Süd oder Safmarine, die dafür sorgen, dass Häfen oder Behörden ebenfalls TradeLens nutzen. Des Weiteren sind die Trustanchors auch die Betreiber der Blockchain-Knoten und stellen sicher das ein Konsens erreicht wird. Zudem speichern die Trustanchors auch die ganze Blockchain bei sich ab. Dies ist vertraglich geregelt [Grä21]. Dabei nutzt TradeLens eine abgewandelte Form des Distributed Ledgers von Bitcoin; nämlich ein Hyperledger Fabric (Permissioned-Blockchain). Diese Form eines Ledgers ist eine unternehmensorientierte Distributed-Ledger-Plattform, bei der selbst bestimmt werden kann, welcher Netzwerkteilnehmer Daten einsehen können oder der Blockchain beitreten dürfen. Eine wichtige Rolle spielen die Smart Contracts. Sie sind für die Dokumentation von

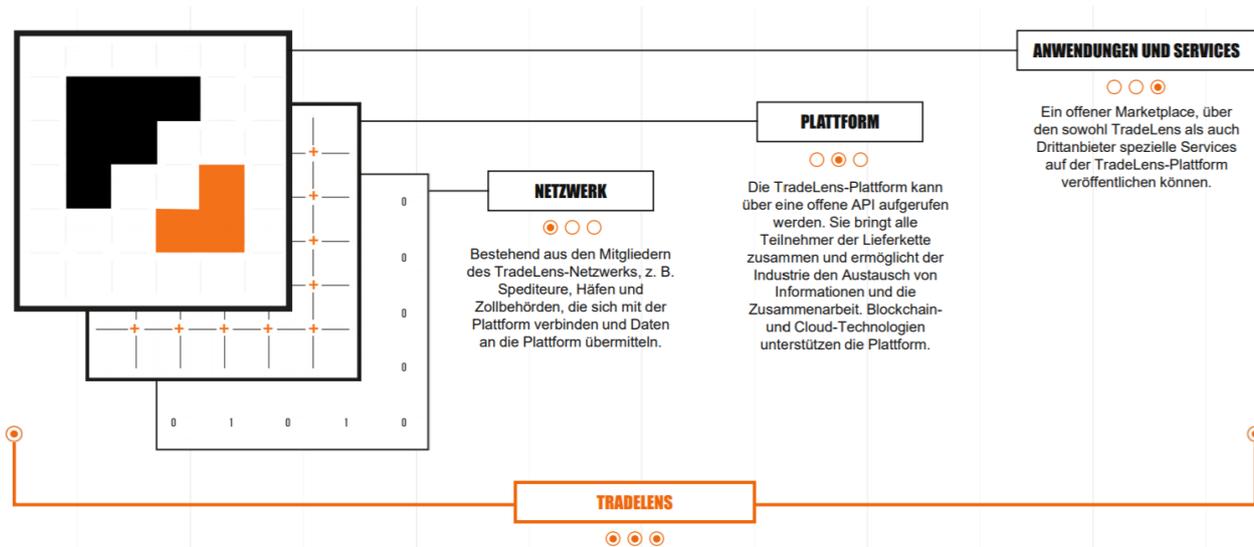


Abbildung 4. Die TradeLensLösung [IBM19]

Geschäftsprozessen verantwortlich und führen Bedingungen zwischen mehreren Parteien aus. Die Smart Contracts sind auf der Blockchain gespeichert und somit unveränderlich und dezentral. Dadurch sind Transaktionen nachverfolgbar und unumkehrbar, was das Vertrauen zwischen den Unternehmen stärkt. Nutzer des Hyperledger Fabric können schnellere Entscheidungen treffen und somit Zeit und Kosten sparen [IBMHL].

Da die Netzwerkteilnehmer in TradeLens bekannt sind, wird kein Mining betrieben. Sie vertrauen sich gegenseitig. Die Blöcke, die für die Blockchain erstellt werden, werden von der IBM Blockchain-Lösung überprüft und angehängen. Der Service von IBM übernimmt die Aufgaben des Miners und kontrolliert neben dem bereits erwähnten auch, dass keine Partei den Blockchain-Verlauf ändert. Aus diesem Grund kann behauptet werden, dass es sich bei TradeLens um keine richtige Blockchain-Anwendung handelt, da sie nicht dezentral ist. IBM könnte die Blockchain umschreiben. Jedoch ist vertraglich geregelt, welche Befugnisse IBM hat. In Sachen Kryptografie nutzt TradeLens ebenfalls die Hashfunktion und die Public-Key-Kryptografie (aber nicht in dem Maße wie Bitcoin [Grä21]). Die Hashfunktion wird vor allem genutzt, um Daten eindeutig zu erkennen. Werden Daten in die Blockchain geschrieben, so werden sie mit einem kryptografischen Hash versehen. Der Hash dient dazu die Datei im Nachhinein wieder zu erkennen [IBM19]. Die Public-Key-Kryptografie wird auch genutzt. Jedoch konnte nicht festgestellt werden, wo sie zum Einsatz kommt.

3.1.2 TRADELENS IN DER PRAXIS

Wie TradeLens in der Praxis funktioniert lässt sich an Abbildung 5 nachverfolgen. In dieser Abbildung ist zu erkennen, welche verschiedenen Stationen eine Lieferung durchlaufen kann. In Abbildung 5 startet der Transport mit der Auslieferung des leeren Containers aus dem Lager. Anschließend durchläuft der Container eine Vielzahl von

Knotenpunkten. TradeLens bietet über 120 Sendungsver-sand-Ereignisse (Meilensteine). Diese Ereignisse reichen von „Container versiegelt“ bis zu „Leerer Container zur Abholung bereit“. Die Meilensteine können in Echtzeit auf TradeLens eingesehen werden und werden kryptografisch auf der Blockchain gespeichert. Für eine Nachverfolgung wird eine Buchungsnummer, eine Gerätenummer oder eine Frachtbriefnummer benötigt. Ist ein Meilenstein erreicht wird über einen Smart Contract alle Teilnehmer der Supply Chain benachrichtigt und das Ereignis auf der Blockchain gespeichert. Ebenfalls befinden sich auf TradeLens über 18 Handelsdokumente, auf die jederzeit zugegriffen werden kann. Durch sie ist möglich beispielsweise Import- und Exportdokumente bereits im Voraus auszufüllen und auf TradeLens hochzuladen. Dadurch können Behörden im Voraus überprüfen, ob die Dokumente korrekt sind und sich Zeit bei der Abwicklung sparen. TradeLens hat seine Stärken bei unvorhergesehenen Ereignissen, wie zum Beispiel bei einer ungeplanten Entladung des Containers. Ein solches Ereignis wird sofort als Meilenstein für alle Parteien sichtbar. Die Unternehmen, die für den weiteren Transport zuständig sind, können auf die Verzögerung reagieren und erfahren davon nicht erst am Übergabeort.

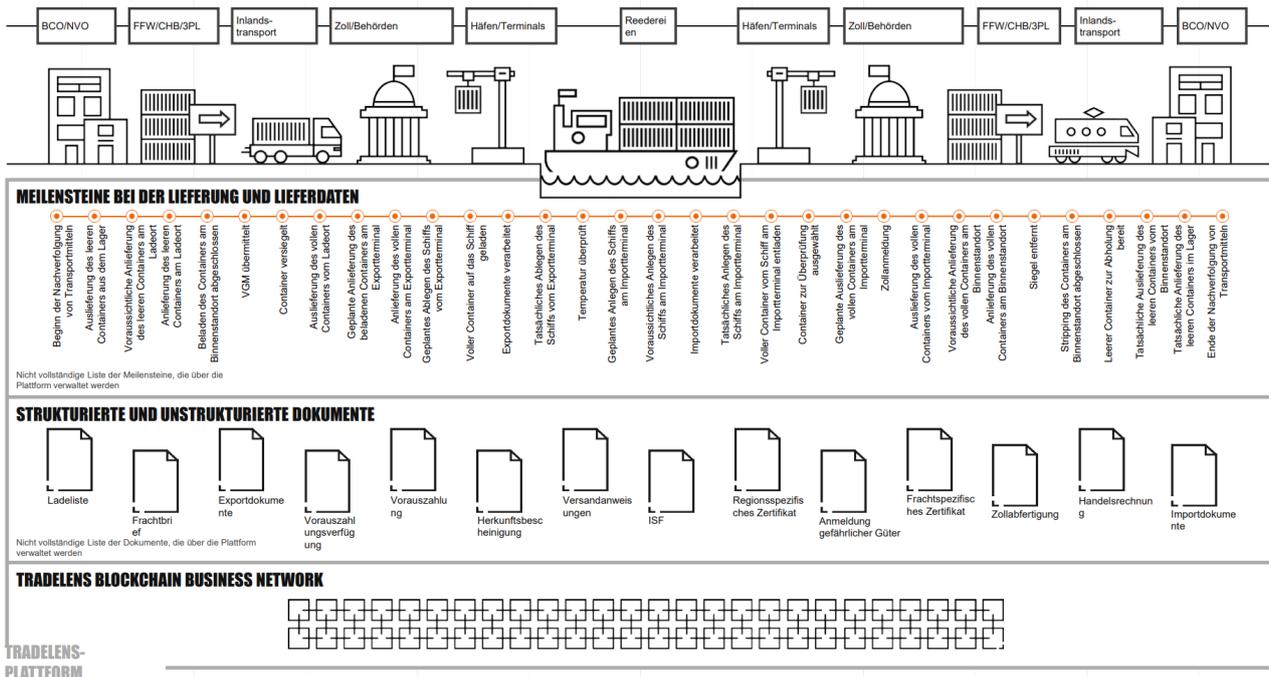


Abbildung 5. Ein Versandbeispiel von TradeLens [IBM19]

3.2 IBM FOOD TRUST

FoodTrust ist ein Cloud-Netzwerk auf Blockchain-Basis für Händler, Lieferanten, Produzenten und Anbieter in der Lebensmittelindustrie. Aktuell gibt es über 110 Mitglieder, von großen Supermarktketten bis zum kleinen Farmer, auf der Plattform. Die Mitglieder teilen untereinander Daten, um eine höhere Nachverfolgbarkeit, Transparenz und Effizienz zu ermöglichen. FoodTrust wurde im Jahr 2016 von IBM und Walmart gegründet. Über die Jahre kamen weitere bekannte Lebensmittelhersteller wie Nestle, Unilever und Dole hinzu. Die Intention von IBM und Walmart ist es Lebensmittelkrisen, wie den E.coli Ausbruch im Jahr 2006 in USA durch Spinat oder den Pferdefleischskandal im Jahr 2013 in Europa, zu verhindern. All diese Krisen entstanden durch fehlende Transparenz und Nachverfolgbarkeit. Die Lebensmittelbehörde in den USA brauchte zwei Wochen für die Aufklärung, der Ursache des E.coli Ausbruches. Für den nationalen Ausbruch war eine Farm mit einer verunreinigte Tagesproduktion verantwortlich [YT17]. Neben den beiden Hauptproblemen krankt die Lebensmittelindustrie noch an weiteren Schwierigkeiten. Wichtige Daten werden von den einzelnen Unternehmen nur auf Anfrage herausgegeben. Der Informationsaustausch zwischen Partnern in einem Bundesstaat funktioniert. Kommt der Partner aus einem anderen Bundesstaat oder aus einem anderen Land, sind Zeit und Geld erforderlich, um Kontakt aufzunehmen. Viele Transaktionen basieren immer noch auf Papier, was ineffizient ist und Spielraum für betrügerische Handlungen gibt. Jedes Unternehmen hat seine eigenen Aufzeichnungen über Transaktionen. Ein Abgleich unterschiedlicher Daten erfordert wieder Zeit und Ressourcen [YT20].

Durch FoodTrust, einer unabhängigen Blockchain-basierenden Plattform, die den Datenaustausch anbietet, können die Teilnehmer dem System vertrauen. Sind Daten auf FoodTrust hochgeladen, hat jeder sofortigen Zugriff auf die Transaktionen, für die er eine Berechtigung hat. Durch die Speicherung der Transaktionen auf der Blockchain sind die Daten unveränderlich. Dadurch wird eine überprüfbare Aufzeichnung aller Transaktionen möglich, was betrügerisches Verhalten verhindert. FoodTrust schafft es aus einem Netzwerk, in dem jeder mit jedem kommunizieren muss, um an Informationen zu bekommen, ein Netzwerk zu schaffen, in dem Informationen auf einer Plattform geteilt werden und für jeden zugänglich sind (siehe Abbildung 6) [YT20].

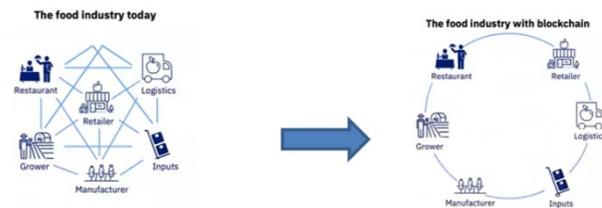


Abbildung 6. Vergleich zwischen der Lebensmittelindustrie ohne Blockchain zur Lebensmittelindustrie mit Blockchain [YT20]

3.2.1 AUFBAU VON FOODTRUST

FoodTrust ist ähnlich aufgebaut wie TradeLens. Beide Plattformen nutzen das Hyperledger Fabric von IBM; eine Technologie, die auf Basis von Open Source in der Linux Foundation entwickelt wurde. Bei dem Hyperledger Fabric

handelt es sich um eine Privat oder Permissioned Blockchain und nicht um eine Public Blockchain [IBMFT].

Des Weiteren werden offene Standards und APIs genutzt, damit auch Mittelständler einfach und ohne viel Aufwand ihre IT anbinden können. IBM FoodTrust verfügt über eine große Palette an APIs. APIs steht für „Application Programming Interface“ und bezeichnet Programmierschnittstellen. Sie sind „ein Satz von Befehlen, Funktionen, Protokollen und Objekten, die Programmierer verwenden können, um eine Software zu erstellen oder mit einem externen System zu interagieren“ [Tal21]. APIs sind wie Legosteine. Sie bilden eine Grundlage von Standardbefehlen auf denen Entwickler Codes schreiben können. Durch Programmierschnittstellen ist es möglich, dass Anwendungen untereinander in Kontakt treten können. Sie werden auf der Blockchain gespeichert, da sie wie Smart Contracts nur Codes sind, die dem Nutzer helfen sollen, Codes selbst zu schreiben. FoodTrust teilt ihre APIs in primäre Client-Anwendungsfälle und Integration von Drittanbieter auf. Zu den primären Client-Anwendungsfällen zählen die Verbraucherverpflichtung und das Lieferkettenmanagement und zu den Integrationen von Drittanbieter zählen Industriegruppen-Anwendungen und Temperatur-Überwachung dazu [Tal21].

Auch FoodTrust nutzt sog. Trustanchors, die für die Konsensfindung verantwortlich sind. Sie sind nicht bekannt. Jedoch kann angenommen werden, dass große Supermarktketten, wie Walmart als Trustanchors fungieren. In den weiteren Punkten wie der Kryptografie und dem Mining gibt es keine wesentlichen Unterschiede zu TradeLens.

3.2.2 FOODTRUST IN DER PRAXIS

IBM FoodTrust eignet sich besonders gut für die Nachverfolgung von Lebensmitteln. Erkennt beispielsweise ein Discounter, dass das Rinderfleisch verschimmelt ist, so kann leicht herausgefunden werden, welcher Teil der Supply Chain dafür verantwortlich ist. Dafür muss nur in der FoodTrust-Oberfläche Rinderfleisch eingegeben werden und sofort findet der Discounter alle Zulieferer von Rinderfleisch. Anschließend kann das Fleisch ausgewählt werden, bei dem der Schimmelbefall aufgetreten ist. Über FoodTrust kann die ganze Lieferkette auf einer Seite überblickt werden. Es kann herausgefunden werden von welchem Bauernhof das Fleisch kommt, wer die Tiere geschlachtet hat, wo es in Hackfleisch oder andere Fleischprodukte verarbeitet und sogar wo es zwischengelagert wurde. All diese Daten können mit genauem Datum auf FoodTrust eingesehen werden. Durch die Speicherung der Daten auf der FoodTrust Blockchain kann diesen Informationen vertrauenswürdig. Der Schlachthof kann nicht abstreiten, dass er das Fleisch zu lange liegen gelassen hat oder die entsprechenden Dokumente fälschen.

FoodTrust und TradeLens nutzen die gleiche Blockchain-Technologie. Jedoch haben sich beiden

Anwendungen auf unterschiedliche Prozesse konzentriert. TradeLens versucht vor allem die bürokratischen Transaktionsprozesse zwischen den unterschiedlichen Parteien in der Supply Chain zu verbessern. FoodTrust hingegen legt sein Hauptaugenmerk auf die Verbesserung einer lückenlosen Rückverfolgung

4 FAZIT

Das Ziel dieser Arbeit war es herauszuarbeiten, welche Transaktionsprozesse können im Bereich der Produktion und Logistik durch den Einsatz der BCT verbessert werden. Anhand von zwei Blockchain-Anwendungen wurde die Forschungsfrage untersucht. Zu Beginn dieser Thesis wurde eine theoretische Grundlage erarbeitet, in der das Themengebiet der Blockchain-Technologie untersucht und beschrieben wurde. Zur spezifischeren Untersuchung wurden das umfangreiche Thema der Blockchain in Unterkategorien aufgeteilt, die eine exaktere Beschreibung der Thematik ermöglichen. Als erstes wurde die Kryptografie in der Blockchain behandelt. Sie baut auf den zwei Säulen Public-Key-Kryptografie und Hashfunktion auf. Anschließend wurde das Mining genauer untersucht. Es konnte festgestellt werden, dass es eine Blockchain wie ein Peer-to-Peer Netzwerk funktioniert. Jedoch haben die Teilnehmer unterschiedliche Aufgaben. Des Weiteren wurden die Konsensmechanismen behandelt. Sie unterscheiden sich je nach Anwendung in der Konsensfindung. Die letzte Unterkategorie im Bereich Blockchain sind die Smart Contracts. Sie sind für die automatische Ausführung von vorher definierten Bedingungen zuständig. Im Hauptteil der Arbeit wurden die beiden Blockchain-basierten Plattformen TradeLens und FoodTrust genauer betrachtet. Es wurde jeweils der Aufbau, die Funktionsweise und die Praxisanwendung beschrieben. TradeLens und FoodTrust sind Blockchain-Projekte, die in Zukunft zum Alltag in der Logistik und Produktion gehören werden. Schon jetzt schaffen es Blockchain-basierte Plattformen, wie diese beiden, eine Menge von Transitionsprozessen zu verbessern. Durch sie kann eine lückenlose Rückverfolgung gewährleistet und die Fälschung von Dokumenten verhindert werden. Zudem schaffen sie es, dass sich Teilnehmer in der Supply Chain durch die Blockchain gegenseitig vertrauen können.

TradeLens und FoodTrust bieten neben den bereits erwähnten Verbesserungen auch Problempunkte, die beachtet werden müssen. Als Nutzer einer solchen Plattform muss immer die Qualität der Informationen berücksichtigt werden. Denn „was in der Blockchain steht muss nicht immer richtig sein. Es kann nur gesagt werden, dass was in der Blockchain steht, wurde nicht verändert“ [Grä21]. Eine Blockchain braucht Technologien, die sie mit exakten Informationen füttert. Hat eine Blockchain-basierte Plattform diese Technologien, kann sie nicht nur Transaktionsprozesse verbessern, sondern auch das Gegenseitige Vertrauen stärken.

Autor	Titel	Zeitschrift	Zusammenfassung
Hans-Georg Fill, Felix Härer, Andreas Meier	Wie funktioniert Blockchain?	Springer Buch (Blockchain-Grundlagen, Anwendungsszenarien und Nutzenpotenziale)	Diese Publikation konzentriert sich auf die Grundlagen der Blockchain und versucht diese einfach zu erklären.
Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, Jinyu Zhang	A Blockchain-based Supply Chain Quality Management Framework	The Fourteenth IEEE International Conference on e-Business Engineering	In diesem Artikel geht es um ein intelligentes Qualitätsmanagement der Lieferketten auf Basis der Blockchain.
Gurudutt Nayak, Amol S. Dhaigude	A conceptual model of sustainable supply chain management in small and medium enterprises using blockchain technology	Cogent Economics and Finance	Der Artikel befasst sich mit einem Modell zum nachhaltigen Supply Chain Management für kleine und mittlere Unternehmen mit Hilfe der Blockchain-Technologie.
Zeinab Shahbazi, Yung-Cheol Byun	Smart Manufacturing Real-Time Analysis Based on Blockchain and Machine Learning Approaches	Applied sciences	In diesem Artikel wird die Verknüpfung von IoT, maschinelles Lernen und Blockchain-Technologie zur Echtzeit-Überwachung von Produktionssystemen behandelt.
Satoshi Nakamoto	Bitcoin: A Peer-to-Peer Electronic Cash System	www.bitcoin.org	In dieser Arbeit wird zum ersten Mal die Nutzung von P2P Netzwerken und Konsensmechanismen beschrieben, um digitales Geld zu transferieren.
Mehrdokht Pourmader, Yangyan Shi, Stefan Seuring, S.C. Lenny Koh	Blockchain applications in supply chains, transport and logistics: a systematic review of the literature	International Journal of Production Research	Diese Abhandlung beschreibt die neusten akademischen Ergebnisse in Sachen Blockchain, IoT und KI. Dabei liegt der Fokus auf Supply Chain Management, Transport und Logistik.
Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou	Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment	Logistics	Dieses Papier liefert durch seine Methodik eine detaillierte Analyse der Blockchain in der Lieferkettenindustrie.
Yingli Wang, Paul Beynon-Davies, Jeong Hugh Han	Understanding blockchain technology for future supply chains: a systematic literature review and research agenda	Supply Chain Management	Dieser Artikel untersucht, wie die Blockchain-Technologie in Zukunft die Lieferketten durch neue Praktiken und Strategien beeinflusst.
Witold Nowinski, Mikos Kozma	How Can Blockchain Technology Disrupt the Existing Business Models?	Entrepreneurial Business and Economics Review	Der Artikel befasst sich damit wie sich die Blockchain auf aktuelle Geschäftsmodelle auswirken kann.
Christoph Meinel, Tatiana Gayvoronskaya	Blockchain – Hype oder Innovation	Springer Buch	Dieses Buch konzentriert sich auf die Vorteile der Blockchain-Technologie im Vergleich zu bereits vorhandenen Lösungen
Archana A Mukherjee, Rajesh Kumar Singh, Ruchi Mishra, Surajit Bag	Application of blockchain technology for sustainability development in agricultural supply chain: justification framework	Operations Management Research	Dieses Papier befasst sich mit den Vorteilen von Blockchain im Lieferkettenmanagement der Agrarindustrie.
Joash Mageto, Rose Luke	Skills frameworks: A focus on supply chains	Journal of Transport and Supply Chain Management	Die Studie dokumentiert und fasst verschiedene Supply Chain Fähigkeiten aus der Literatur zusammen, um als Leitfaden zu dienen.
Thoma Jensen, Niels Bjorn-Andersen, Ravi K. Vatrappu	Avocados crossing borders: The problem of runway objects and the solution of a shipping information pipeline for improving international trade	Information Systems Journal	Der Artikel veranschaulicht die Herausforderungen von Containertransporten von Afrika nach Europa.
Johannes Lehner, Phillip Schützeneder, Johannes Sametinger	Custom Tokens und Smart Contracts zur Projektsteuerung	Springer Buch (Blockchain-Grundlagen, Anwendungsszenarien und Nutzenpotenziale)	Diese Publikation beschreibt und erklärt die Grundlagen zu Custom Tokens und Smart Contracts.

Tabelle 3. Bedeutende Publikationen zum Forschungsthema

LITERATUR

- [Car20] Cardano; The Blockchain Revolution Started With Bitcoin. It Continues Now With Ouroboros. Online verfügbar unter <https://cardano.org/ouroboros/#proof-of-stake>, zuletzt geprüft am 14.11.2021.
- [FHM20] Fill, Hans-Georg; Härer, Felix; Meier, Andreas; Wie funktioniert die Blockchain., in: Fill, H-G./Meier, A. (Hrsg.): Blockchain – Grundlagen, Anwendungsszenarien und Nutzungspotenziale, Springer Verlag, Deutschland, Wiesbaden, 2020. - ISBN 978-3-658-28005-5.
- [LSS20] Lehner, Johannes; Schützeneder, Philipp; Sametinger, Johannes; Custom Tokens und Smart Contracts zur Projektsteuerung., in: Fill, H-G./Meier, A. (Hrsg.): Blockchain – Grundlagen, Anwendungsszenarien und Nutzungspotenziale, Springer Verlag, Deutschland, Wiesbaden, 2020. - ISBN 978-3-658-28005-5.
- [MG20] Meinel, Christoph; Gayvoronskaya, Tatiana: Blockchain – Hype oder Innovation: Springer Verlag, Berlin, Deutschland, 2020. - ISBN 978-3-662-61915-5.
- [NK17] Nowinski, Witold; Kozma, Miklos: How can Blockchain Technology Disrupt the Existing Business Models?, in: Entrepreneurial Business und Economics Review, Vol. 5, Nr. 3, 2017.
- [PSSK19] Mehrdokht, Pournader; Yangyan, Shi; Stefan, Seuring; S.C. Lenny, Koh: Blockchain applications in supply chains, transport and logistics: a systematic review of the literature, In: International Journal of Production Research Vol. 58, Nr. 7, 2019.
- [Sch19] Schiller, Kai; Was ist Proof-of-Importance und wie funktioniert es? Online verfügbar unter <https://blockchain-welt.de/proof-of-importance-poi/>, zuletzt geprüft 13.11.2021.
- [WHB19] Wang, Yingli; Han, Jeong Hugh; Beynon-Davies, Paul: Understanding blockchain technology for future supply chains: a systematic literature review and research agenda, in: Supply Chain Management: An International Journal, Vol. 24, Nr. 1, 2019.
- Grä21 Gräfe, Michael (Director of Supply Chain Transformation, IBM); persönliches Interview, via Zoom-Call, 09.06.2021.
- Hay18 Hays, Demelza; Smart Contracts. Online verfügbar unter <https://cryptoresearchreport.de/crypto-research/smart-contracts/>, zuletzt geprüft 14.11.2021.
- IBM19 IBM; TradeLens Überblick. Online verfügbar unter <https://www.ibm.com/downloads/cas/1ZVRWXPG>, zuletzt geprüft 15.11.2021.
- IBMFT IBM; IBM Food Trust: Eine neue Ära in der Lebensmittelversorgung der Welt; Online verfügbar unter <https://www.ibm.com/de-de/blockchain/solutions/food-trust>, zuletzt geprüft 15.11.2021.
- IBMHL IBM; Was ist Hyperledger Fabric; Online verfügbar unter <https://www.ibm.com/de-de/topics/hyperledger>, zuletzt geprüft 15.11.2021.
- Tal21 Talend; API; Online verfügbar unter <https://www.talend.com/de/resources/was-ist-eine-api/>, zuletzt geprüft 15.11.2021.
- YT17 YouTube; Online verfügbar unter https://www.youtube.com/watch?v=MMOF0G_2H0A&t=760s, zuletzt geprüft 15.11.2021.
- YT19 YouTube; Online verfügbar unter https://www.youtube.com/watch?v=Xwqo_fwPEJo&t=24s, zuletzt geprüft 15.11.2021.
- YT20 YouTube; Online verfügbar unter <https://www.youtube.com/watch?v=rkJT-Z8-8w&t=2s>, zuletzt geprüft 15.11.2021.

Simeon Eberlein, B.Eng., geb. 1998, Wissenschaftlicher Mitarbeiter am Lehrstuhl Produktionswirtschaft an der Brandenburgisch Technischen Universität Cottbus-Senftenberg,

Univ.-Prof. Dr. habil. Herwig Winkler, geb. 1973, Inhaber des Lehrstuhls für Produktionswirtschaft an der Brandenburgisch Technischen Universität Cottbus-Senftenberg,

Adresse: BTU Cottbus-Senftenberg, Lehrstuhl für Produktionswirtschaft, Siemens-Halske-Ring 6, 03046 Cottbus, Deutschland