Bachelorarbeit

Kritische Betrachtung ausgewählter Einsatzgebiete der Blockchain-Technologie unter besonderer Berücksichtigung des Supply-Chain-Managements

Titel der Arbeit

Simon van Unen, Gelsenkirchen

Name, Geburtsort

Wirtschaft

Studiengang

Wirtschaft

Fachbereich

Westfälische Hochschule Gelsenkirchen

Hochschule

Prof. Dr. Küffmann

Erstprüferin/Erstprüfer

Prof. Dr. Propach

Zweitprüferin/Zweitprüfer

25.10.2018

Abgabedatum

Inhaltsverzeichnis

Inhaltsverzeichnis II

Abkürzungsverzeichnis IV

Abbildungsverzeichnis V

Tabellenverzeichnis VI

1. Einleitung 1

1.1 Problemstellung und Zielsetzung 1

1.2 Aufbau der Arbeit 2

2. Definitionen 4

2.1 Blockchain 4

2.2 Distributed Ledger Technology 4

2.3 Supply-Chain-Management 5

2.4 Smart Contract 5

2.5 Bitcoin 6

3. Kryptographie 7

3.1 Hash Funktionen 8

3.1.1 Einwegfunktion 8

3.1.2 Kollisionsresistenz 9

3.1.2.1 Urbild-Kollisionsresistenz 9

3.1.2.2 Zweite-Urbild-Resistenz 10

3.1.3 SHA-256 10

3.2 Digitale Signaturen 11

4. Blockchain 13

4.1 Öffentliche/Private Blockchain 13

4.2 Dezentralisierung 14

4.3 Blöcke und Blockchain 15

4.4 Group Consensus 17
4.4.1 Proof of Work 17
4.4.2 Proof of Stake 19
5. Supply-Chain-Management 20
5.1 Probleme des SCM 21
5.1.1 Globalisierung 21
5.1.2 Echtzeit-Informationsstand 21
5.1.2.1 Ripple-Effekt 22
5.1.2.2 Bullwhip-Effekt 22
5.1.3 Compliance und Qualität 24
5.1.4 Vertrauen 24
5.2 Blockchain-Technologie im SCM 25
5.2.1 IOT-Ebene 26
5.2.2 Unternehmen-Ebene 28
5.2.2.1 Transparenz der Blockchain 28
5.2.2.2 Vertrauen 29
5.2.2.3 Betrug 31
5.2.3 Smart Contract-Ebene 32
5.2.4 Unternehmens-Ebene 34
5.3 Anwendungsbeispiel E. coli 35
5.4 Kritik 38
6. Blockchain im Gesundheitswesen 40
7. Fazit 42
Literatur- und Quellenverzeichnis 44
Eidesstattliche Versicherung 49

Abkürzungsverzeichnis

DL	Distributed Ledger
GPS	Global Positioning System
IOT	Internet of Things
RFID	Radio Frequency Identification
SCM	Supply-Chain-Management
u.a.	unter anderem
URL	Uniform Resource Locator
Vgl.	vergleiche
z.B.	zum Beispiel

Abbildungsverzeichnis

Abbildung 1: Urbild-Kollisionsresistenz 9
Abbildung 2: Zweite-Urbild-Resistenz 10
Abbildung 3: SHA-256 11
Abbildung 4: Unterschied zentralisierte/verteilte Datenbank 14
Abbildung 5: Hash-Baum 15
Abbildung 6: Blockchain 16
Abbildung 7: Entstehung des Header Hashes 18
Abbildung 8: Bullwhip-Effekt 23
Abbildung 9: SCM Blockchain Konstrukt 25
Abbildung 10: IOT-Ebene 27
Abbildung 11: Beispiel Smart Contract 32
Abbildung 12: Zusammenspiel der drei Ebenen 33
Abbildung 13: Der Weg des Spinates 36

Tabellenverzeichnis

Tabelle 1: Vergleich öffentliche/private Blockchain 13
Tabelle 2: Vergleich traditionelles Track&Trace mit der Blockchain 39

1. Einleitung

1.1 Problemstellung und Zielsetzung

In der heutigen Zeit spielen der technologische Fortschnitt und die technologische Innovation eine große Rolle. Immer schneller werden neue Technologien entwickelt und es ist eine Herausforderung auf dem neusten Stand der Technik zu bleiben. Die Blockchain-Technologie ist eine dieser neuen Technologien. Sie ist noch eine sehr junge Technologie und wird stets weiterentwickelt. Die meisten Menschen assoziieren mit dem Begriff „Blockchain“ Bitcoin. Dies ist auch korrekt, da Bitcoin die Geburt der Blockchain-Technologie war. Jedoch hat die Blockchain-Technologie das Potential in vielen weiteren Anwendungsfeldern Fuß zu fassen.

Eines dieser Anwendungsfelder ist auch die Verbesserung des Supply-Chain-Management. Das SCM profitiert seit jeher von den neusten Entwicklungen, sei es im Bereich der Kommunikation oder des Transportes. Jedoch steht das SCM vor immer neuen Herausforderungen. Heutzutage wird eine Vielzahl von Gütern aus dem Ausland und oft von Übersee importiert. Das erschwert für den Kunden oder Käufer den wahren Wert eines Produktes zu erkennen, denn es fehlt oft die Transparenz entlang der gesamten Wertschöpfungskette.

Durch Globalisierung und Import gibt es eine große Anzahl von Kontaktpunkten in der Wertschöpfungskette. Es ist schwer den Ursprung vieler Produkte sowie deren aktuellen Aufenthaltsort zu eruieren. Bei vielen Produkten bleibt der Kunde über deren Herkunft im Unwissenden und kann somit nicht erkennen, ob sie zum Beispiel unter ethisch korrekten Verhältnissen produziert wurden.

Durch die Blockchain-Technologie besteht die Möglichkeit Klarheit in diese Felder zu bringen. Mit ihrer Hilfe kann der gesamte Prozessweg für jedermann offengelegt und verfolgbar gemacht werden. Dies würde das Vertrauen aller Teilnehmer erhöhen und Betrug verringern.

Des Weiteren ist das Bearbeiten von Verträgen und weiteren Dokumenten auf herkömmliche Weise sehr zeitaufwändig und kann das SCM beeinträchtigen. Auch in diesem Bereich bietet die Blockchain-Technologie Lösungsvorschläge an.

Die Blockchain-Technologie hat die Möglichkeit auch außerhalb des SCM Anwendung zu finden. Das Gesundheitswesen ist eines dieser Anwendungsfelder in welchem Implementierungspotential besteht.

Daher ist das Ziel dieser Arbeit eine Einführung in die Blockchain-Technologie und ihren technischen Hintergrund zu gewähren und ihr zukünftiges Potential in ausgesuchten Anwendungsfeldern, mit besonderem Blick auf das SCM, darzustellen. Anhand von ausgewählten Bewertungskriterien eines erfolgreichen SCM wird dargestellt, ob die Blockchain einen festen Platz im SCM finden wird.

1.2 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in sieben Abschnitte.

In dem ersten Abschnitt werden zentrale Begriffe definiert, welche benötigt werden, um die vorliegenden Texte zu verstehen.

Daraufhin findet eine Einführung in die Kryptographie statt. In ihr werden Hashfunktionen und digitale Signaturen erläutert. Dies ist notwendig, da die Blockchain-Technologie sich auf diese kryptographischen Verfahren beruft.

Mit Hilfe des vorherigen Kapitels wird im dritten Abschnitt die Blockchain-Technologie und ihre Funktionsweise dargestellt. Sie bildet die Grundlage für die folgenden Kapitel.

Bevor dargestellt werden kann, wie die Blockchain-Technologie im Supply Chain Management verwendet werden kann, findet zunächst, im vierten Abschnitt, eine grundlegende Einführung in das SCM statt. In dieser werden Erfolgskriterien für ein erfolgreiches SCM aufgeführt und die heutigen Probleme des SCM dargestellt.

Im fünften Abschnitt wird erklärt, wie die Blockchain-Technologie in ein SCM-System integriert werden kann und wie sie dabei hilft, die vorher erläuterten Probleme zu beseitigen. An einem Fallbeispiel aus dem Jahre 2006 wird ihr Potential und die Einsatzmöglichkeiten verdeutlicht. Darauf folgt eine kritische Betrachtung der Blockchain-Technologie im SCM.

Da die Blockchain-Technologie auch außerhalb des SCM eingesetzt werden kann, wird im sechsten Abschnitt kurz erklärt, wie die Blockchain-Technologie in das Gesundheitswesen integriert werden kann.

Der letzte Abschnitt beinhaltet das Fazit, welches sich auf die Problemstellung bezieht. Die im vierten Abschnitt aufgeführten Erfolgskriterien für ein Erfolgreiches SCM werden in diesem Abschnitt beurteilt.

2. Definitionen

Um die vorliegende Arbeit zu verstehen, müssen zunächst bestimmte Grundbegriffe erläutert werden.

2.1 Blockchain

Eine offizielle anerkannte Definition für die Blockchain ist noch nicht vorhanden, da die Technologie sich stets weiterentwickelt und ändert. In der vorliegenden Arbeit wird folgende Definition als Grundlage verwendet:

„Technisch stellt die Blockchain ("Blockkette") eine dezentrale Datenbank dar, die im Netzwerk auf einer Vielzahl von Rechnern gespiegelt vorliegt. Die Authentizität der einzelnen Datenbankeinträge wird dabei durch einen aus dem Netzwerk hergestellten Konsensmechanismus sichergestellt. Aufgrund ähnlicher Charakteristika wird der Begriff „Distributed Ledger“ oftmals synonym verwendet, auch wenn nicht jeder Distributed Ledger unbedingt eine Blockkette verwendet.“[1]

2.2 Distributed Ledger Technology

Die Blockchain ist eine Variante des Distributed Ledger, zu Deutsch: „dezentrales/verteiltes Kontobuch“.

„Bei der Distributed Ledger Technologie (DLT) handelt es sich um eine spezielle Form der elektronischen Datenverarbeitung und -speicherung. Als Distributed Ledger oder „Verteiltes Kontenbuch“ wird eine dezentrale Datenbank bezeichnet, die Teilnehmern eines Netzwerks eine gemeinsame Schreib- und Leseberechtigung erlaubt. Im Gegensatz zu einer zentral verwalteten Datenbank bedarf es in diesem Netzwerk keiner zentralen Instanz, die neue Einträge in der Datenbank vornimmt. Neue Datensätze können jederzeit von den Teilnehmern selbst hinzugefügt werden. Ein

[1] Mitschele, Andreas (2016): Blockchain. [online]. URL: https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-188335 (Abruf: 09.07.2018).

anschließender Aktualisierungsprozess sorgt dafür, dass alle Teilnehmer jeweils über den neuesten Stand der Datenbank verfügen."[2]

2.3 Supply-Chain-Management

Unter Supply-Chain-Management versteht sich der Aufbau und die Verwaltung von Logistikketten.[3] Logistikketten beinhalten Material-, Informations- sowie Geldflüsse der gesamten Wertschöpfungskette. Das SCM erstreckt sich von der Bezugsquelle bis zur Verbrauchsquelle. [4]

2.4 Smart Contract

Im zweiten Teil dieser Arbeit, spielen Smart Contracts eine große Rolle. Daher werden, in der vorliegenden Arbeit Smart Contracts wie folgt definiert:

„Ein Smart Contract ist ein Vertrag auf Software-Basis, bei dem unterschiedlichste Vertragsbedingungen hinterlegt werden können. Während des Vertragsverlaufs können bestimmte verknüpfte Aktionen (z. B. Auszahlungen) selbsttätig ausgeführt werden, wenn ein entsprechender Auslöser (z. B. Erfüllung von Vertragsbedingungen) vorliegt."[5]

---

[2] Metzger, Jochen (2018): Distributed Ledger Technologie (DLT). [online]. URL: https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444 (Abruf: 09.07.2018).

[3] Vgl. Voigt, Kai-Ingo u.a. (2018): Supply Chain Management (SCM). [online]. URL: https://wirtschaftslexikon.gabler.de/definition/supply-chain-management-scm-49361/version-272597 (Abruf: 09.10.2018).

[4] Vgl. Werner, Hartmut (2017): Supply Chain Management Grundlagen, Strategien, Instrumente und Controlling, 6. Auflage, S. 6.

[5] Mitschele, Andreas (2018): Smart Contract. [online]. URL: https://wirtschaftslexikon.gabler.de/definition/smart-contract-54213/version-277263 (Abruf: 09.07.2018).

2.5 Bitcoin

Da Bitcoin der Ursprung der Blockchain ist und in dieser Arbeit viele technische Grundlagen von der Bitcoin-Blockchain erläutert werden, ist es auch wichtig, zu verstehen, um was genau es sich dabei handelt. Der Erfinder von Bitcoin, Satoshi Nakamoto, beschreibt Bitcoin als eine digitale Währung, welche die Peer-to-Peer-Technologie nutzt.[6]

[6] Vgl. Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. [online]. URL: https://bitcoin.org/bitcoin.pdf (Abruf: 22.10.2018).

3. Kryptographie

Da es keine zentrale Kontrolleinheit gibt muss bei einer Blockchain über einen anderen Weg Vertrauen und Sicherheit gewährleistet werden. Dies muss jedoch komplett technologisch gewährleistet werden um ein dezentrales Konstrukt zu bleiben. Hier kommt nun die Kryptografie ins Spiel. Durch sie kann ein sicheres Verschlüsselungsverfahren in die Blockchain selbst integriert werden.

Der Mensch nutzt schon seit der Epoche des Altertums kryptographische Verfahren. In Zeiten des Krieges musste verhindert werden, dass aus vom Feind abgefangenen Nachrichten Informationen gewonnen werden konnten. Um dies zu verhindern wurden alle Nachrichten kryptographisch verschlüsselt und so für den Feind nutzlos gemacht.[7]

Allgemein lässt sich sagen, dass Kryptographie zum Datenschutz verwendet wird, zum Beispiel beim Verschlüsseln von Nachrichten.[8] Das Verschlüsseln von Nachrichten bringt einige Vorteile mit sich. Zum einen wird für Vertraulichkeit gesorgt, da die Bedeutung und der Zweck einer Nachricht verborgen werden. Es lassen sich keine Informationen aus einer verschlüsselten Nachricht entnehmen und die Verschlüsselung lässt sich, ohne geheimen Schlüssel, nicht umkehren. Des Weiteren entsteht Integrität, da alle Teilnehmer sicher sein können, dass die Nachricht sicher von einem Punkt zum anderen kommt, ohne dass ihre Bedeutung geändert werden kann. Authentizität entsteht, da jeder Versender einer kryptografisch verschlüsselten Nachricht auch seine Identität beilegt. Dadurch ist der Empfänger in der Lage dem Versender zu authentifizieren.[9]

In dem folgenden Kapitel werden kryptographische Hash-Funktionen und digitale Signaturen genauer betrachtet.

---

[7] Vgl. Kauffmann, Rémy; Zehnder, Patrick (2017): Geschichte der Kryptographie S. 3. [online]. URL: https://www.swisseduc.ch/geschichte/kryptographie/docs/script_kryptographie_swisseduc.pdf (Abruf: 18.10.2018).

[8] Vgl. Paar, Christof; Pelzl, Jan (2016): Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender S. 2.

[9] Vgl. St Denis, Tom; Johnson, Simon (2017): Kryptografie für Entwickler Das erste umfassende Kryptografie-Handbuch für Software-Entwickler S. 24-30.

3.1 Hash Funktionen

Eine Hash Funktion berechnet aus einer beliebig großen Nachricht eine Bitfolge fester Länge. Der Ausgabewert, der sogenannte „Hash“, ist der Fingerabdruck einer Nachricht.[10]

Hash(Blockchain) = efe3fbaa6db3f43cf45d8ee3fdb168cd448afa41[11]

Damit eine Hash Funktion kryptografisch nützlich sein kann, muss sie folgende Eigenschaften aufweisen:

1. Sie dürfen nur in eine Richtung ablaufen (Einwegfunktion).

2. Sie müssen kollisionsresistent sein.[12]

3.1.1 Einwegfunktion

Unter einer Einwegfunktion versteht sich eine Funktion, welche leicht in eine Richtung zu berechnen ist, die Umkehrfunktion jedoch schwierig zu berechnen ist. Dies bedeutet jedoch nicht, dass es unmöglich sei, eine Einwegfunktion umzukehren. Es ist nur so aufwendig, dass es praktisch nicht umsetzbar ist.[13] Bei einer Hash Funktion soll es also nicht möglich sein, aus einem vorliegenden Hash die Ausgangsnachricht zu bilden.[14] Es dürfen also keine nützlichen Informationen aus der vorliegenden Ausgabe über die Eingabe zu entschlüsseln sein.

---

[10] Vgl. Paar, Christof; Pelzl, Jan (2016): Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender S. 335.
[11] Sha-1 Hash.
[12] Vgl. St Denis, Tom; Johnson, Simon (2017): Kryptografie für Entwickler Das erste umfassende Kryptografie-Handbuch für Software-Entwickler S. 261.
[13] Vgl. Karpfinger, Christian; Kiechele, Hubert (2010): Kryptologie Algebraische Methoden und Algorithmen S. 76.
[14] Vgl. Paar, Christof; Pelzl, Jan (2016): Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender S. 339.

3.1.2 Kollisionsresistenz

Bei einer Hashfunktion ist es dazu noch wichtig, dass zwei verschiedene Eingaben nicht den gleichen Hashwert bilden. Idealerweise sollte es erst gar nicht möglich sein, dass Kollisionen auftreten. Dies ist aber durch das Schubfachprinzip nicht möglich.

Das Schubfachprinzip besagt, dass wenn n Objekte auf m Mengen ($n,m > 0$) verteilt werden und n größer als m ist, es mindestens eine Menge gibt welche sich doppelt.[15]

Da jede Hashfunktion eine feste Ausgangslänge in Bit hat und es unendlich viele Eingabewerte gibt, müssen unterschiedliche Eingabewerte den gleichen Hashwert bilden. Daher muss eine starke Hashfunktion es unmöglich machen, für eine Nachricht M_1 mit Hashwert H_1 eine weitere Nachricht M_2 zu bilden, deren Hashwerte $H_1 = H_2$ übereinstimmen. Es ist möglich, zufällige M_2 zu bilden und dann jeweils die Hashwerte zu vergleichen. Jedoch ist es bei Ausgabenlängen von mindestens 100 Bit sehr unwahrscheinlich mit der heutigen Rechenleistung Kollisionen zu finden.[16]

Eine Hash-Funktion muss zwei Arten von Kollisionsresistenzen aufweisen.

3.1.2.1 Urbild-Kollisionsresistenz

Die Urbild-Kollisionsresistenz besagt, dass es nicht trivial sein soll, zu einem gegebenen Hash Y eine Nachricht M zu finden, welche denselben Hash bildet.

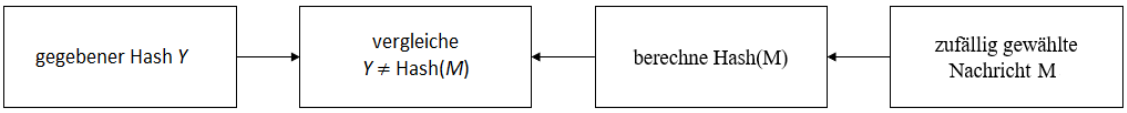

Abbildung 1: Urbild-Kollisionsresistenz

Quelle: Selbsterstellte Abbildung.

[15] Vgl. Schelthoff, Christof (2010): Diskrete Mathematik Diskrete Strukturen & Zahlentheorie S. 13-16.

[16] Vgl. Paar, Christof; Pelzl, Jan (2016): Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender S. 340 f.

3.1.2.2 Zweite-Urbild-Resistenz

Die zweite-Urbild-Resistenz besagt, dass es nicht trivial sein soll, bei einer gegebenen Nachricht M1 eine weitere Nachricht M2 zu finden, welche denselben Hash bilden.[17]

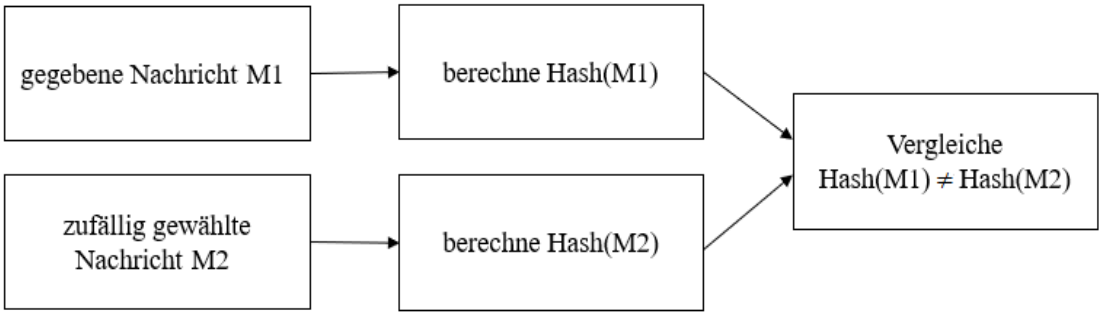

Abbildung 2: Zweite-Urbild-Resistenz

Quelle: Selbsterstellte Abbildung.

3.1.3 SHA-256

Einer der meist verwendeten Hash Algorithmen ist SHA-256, welcher auch bei Bitcoin zum Einsatz kommt.[18] Die Grundlage ist eine kollisionssichere Kompressionsfunktion, welche durch das Anwenden von Merkles Meta-Verfahren eine kollisionssichere Hash-Funktion bildet. Dadurch kann aus einem willkürlich langen Input ein 256 Bit Hashwert erzeugt werden.

Dafür wird der beliebig lange Input in 512 Bit große Blöcke aufgeteilt. Diese Blöcke werden nun, mit einem zuvor berechneten, 256 Bit großen Hashwert des vorherigen Blockes verbunden. Dadurch entsteht ein 768 Bit großer Inputwert, welcher von der Kompressionsfunktion wieder in einen 256 Bit großen Hashwert komprimiert wird. Dieser Hashwert wird nun wieder mit dem nächsten Block verbunden und komprimiert. Da der erste Block nicht mit einem vorherigen Hashwert verbunden werden kann, wird ein Initialisierungsvektor verwendet. Dieser hat einen zufälligen Wert und wird für jedes Dokument verwendet.

---

[17] Vgl. St Denis, Tom; Johnson, Simon (2017): Kryptografie für Entwickler Das erste umfassende Kryptografie-Handbuch für Software-Entwickler S. 261 f.

[18] Vgl. Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System S. 3. [online]. URL: https://bitcoin.org/bitcoin.pdf (Abruf: 22.10.2018).

Der ausgegebene 256 Bit große Hashwert des letzten Blockes, ist der finale Hashwert.[19]

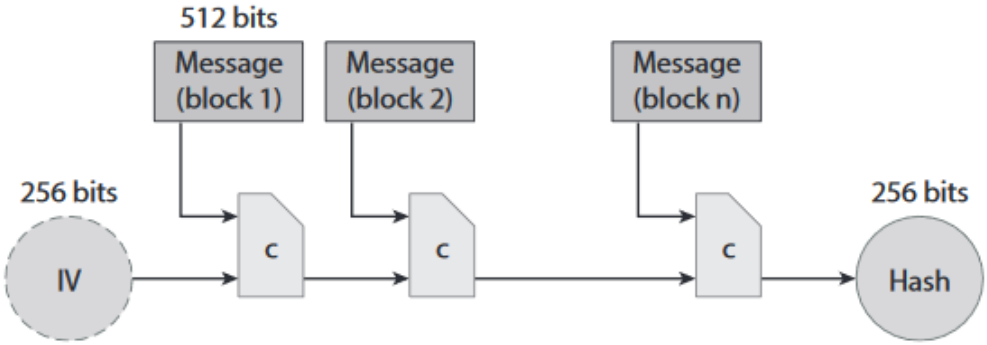

Abbildung 3: SHA-256
Quelle: Narayanan, Arvind u.a. (2016): Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction S. 10.

3.2 Digitale Signaturen

Bei vielen Dokumenten ist es wichtig, dass sie zweifellos zuordbar sind und nicht verfälscht wurden. Da sich viele Prozesse immer weiter digitalisieren, werden auch Unterlagen wie Verträge und Rechnungen digital versendet. Diese benötigen meistens eine handschriftliche Unterschrift. Als Ersatz zu dieser herkömmlichen Methode werden immer mehr digitale Signaturen verwendet. Damit diese digitale Signatur nicht einfach kopierbar ist und somit für andere Dokumente verwendet werden kann, muss die digitale Signatur im Zusammenhang mit dem Dokument stehen. Diese digitale Signatur darf, um gültig zu sein, nicht fälschbar sein und es muss möglich sein, sie auf ihre Echtheit zu überprüfen. Damit die digitale Signatur gültig bleibt, darf das Dokument auch nicht, ohne dass dies an der Signatur erkennbar ist, veränderbar sein.

Dafür hat jeder Nutzer einen privaten Schlüssel und einen öffentlichen Schlüssel. Diese Schlüssel werden unterschiedlich, abhängig von dem verwendeten kryptographischen Verfahren, gebildet.

[19] Vgl. Narayanan, Arvind u.a. (2016): Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction S. 9 f.

Wie der Name schon sagt, wird der private Schlüssel nicht öffentlich zugänglich gemacht und zum Erstellen der digitalen Signatur eines Dokumentes verwendet. Dafür wird die Nachricht mit dem privaten Schlüssel des Erstellers durch eine kryptografische Hashfunktion *f* verschlüsselt. Daraus ergibt sich die digitale Signatur.

f (Nachricht, privater Schlüssel) = digitale Signatur

Nun müssen die anderen Teilnehmer verifizieren können, dass das unterschriebene Dokument auch wirklich von dem Besitzer des privaten Schlüssels kommt. Dafür kommt der öffentliche Schlüssel des Erstellers der digitalen Signatur ins Spiel. Durch den öffentlichen Schlüssel des Erstellers und einem mathematischen Algorithmus *m* lässt sich leicht bestimmen, ob die Nachricht und die digitale Signatur mit dem privaten Schlüssel korrespondieren. [20] [21]

m (Nachricht, Signatur, öffentlicher Schlüssel) = richtig/falsch

Dieser mathematische Algorithmus *m* beweist, dass die Nachricht und die digitale Signatur von dem Besitzer, des zum öffentlichen Schlüssel zugehörigen privaten Schlüssels, stammt.[22] Da der private Schlüssel, nur einer Person bekannt ist, ist dies eindeutig zuordbar.

Dieses System ist nur manipulierbar, indem sich ein dritter Zugang zu dem privaten Schlüssel einer Person bereitet.

[20] Vgl. Karpfinger, Christian; Kiechle, Hubert (2010): Kryptologie Algebraische Methoden und Algorithmen S. 209.
[21] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 39.
[22] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 39.

4. Blockchain

4.1 Öffentliche/Private Blockchain

Es gibt zwei verschiedene Arten von Blockchain, die private und die öffentliche Blockchain. Der Unterschied liegt hier jedoch nicht in der Funktionsweise, welche wir im folgenden Abschnitt kennen lernen. Der Unterschied zwischen den beiden Varianten liegt in den Berechtigungen der verschiedenen Teilnehmer, wer genau die Erlaubnis hat, sich am Netzwerk zu beteiligen und verschiedene Aufgaben zu erfüllen. [23]

Die öffentliche Blockchain ist für alle zugänglich und verwendet meistens einen Open-Source-Code, den die Teilnehmer pflegen. Dadurch sind die Teilnehmer größtenteils unbekannt und nicht unbedingt vertrauensvoll.

Bei der privaten Blockchain hingegen haben nur bestimmte ausgesuchte Personen diese Rechte. Dadurch sind die Teilnehmer bekannt und es wird ihnen vertraut. Jedoch hat dadurch nicht jeder die Möglichkeit, Daten in der Blockchain zu lesen.[24] [25]

Tabelle 1: Vergleich öffentliche/private Blockchain

öffentliche Blockchain	private Blockchain
Teilnehmer sind nicht zwingend bekannt	Teilnehmer sind bekannt
Teilnehmern wird nicht zwingend vertraut	Teilnehmern wird vertraut
Jeder kann ohne Erlaubnis Daten lesen	Kann nur mit Erlaubnis Daten lesen
Jeder kann ohne Erlaubnis Daten eintragen	Kann nur mit Erlaubnis Daten eintragen

Quelle: In Anlehnung an: Morabito, Vincenzo (2017): Business Innovation Through Blockchain, S. 9.

[23] Vgl. Jayachandran, Praveen (2017): The difference between public and private blockchain. [online]. URL: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (Abruf: 09.10.2018).
[24] Vgl. Morabito, Vincenzo (2017): Business Innovation Through Blockchain S. 8 f.
[25] Vgl. Lewis, Antony (2015): A Gentle Introduction To Blockchain Technology S. 6. [online]. URL: https://assets.ctfassets.net/sdlntm3tthp6/1N6VBCrkp6oywIooC20omQ/9b93ac6ac921743a38f80aaeb823a102/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf (Abruf: 09.10.2018).

4.2 Dezentralisierung

Um zu verstehen wie eine Blockchain totale Dezentralisierung erreicht, werden die Begriffe „full node“ und „light node“ benötigt.

Das Netzwerk setzt sich aus mehreren full nodes zusammen. Eine full node ist ein Teilnehmer, welcher das Netzwerk sichert und am Laufen hält, indem er einen bestimmten Algorithmus ausführt. Jede full node besitzt einen Distributed Ledger, welcher eine vollständige Aufzeichnung aller Transaktionen des Netzwerkes enthält.[26] Alle Teilnehmer haben die Möglichkeit eine full node zu betreiben, indem sie ihren Computer diesen bestimmten Algorithmus ausführen lassen. Als Anreiz eine full node zu betreiben, um das Netzwerk aufrecht zu erhalten, gibt es eine Belohnung. Bei der Bitcoin-Blockchain ist diese Belohnung eine bestimmte Anzahl an Bitcoins und die Transaktionskosten.[27]

Light nodes sind hingegen alle Teilnehmer, die keine full nodes sind, jedoch trotzdem das Netzwerk nutzen. So können Transaktionen ausgeführt, empfangen und verfolgt werden, ohne selbst eine full node zu betreiben.[28]

Dadurch ist ein Blockchain-Netzwerk in der Lage auf eine zentrale Kontrolleinheit zu verzichten und komplett dezentral und verteilt zu sein.

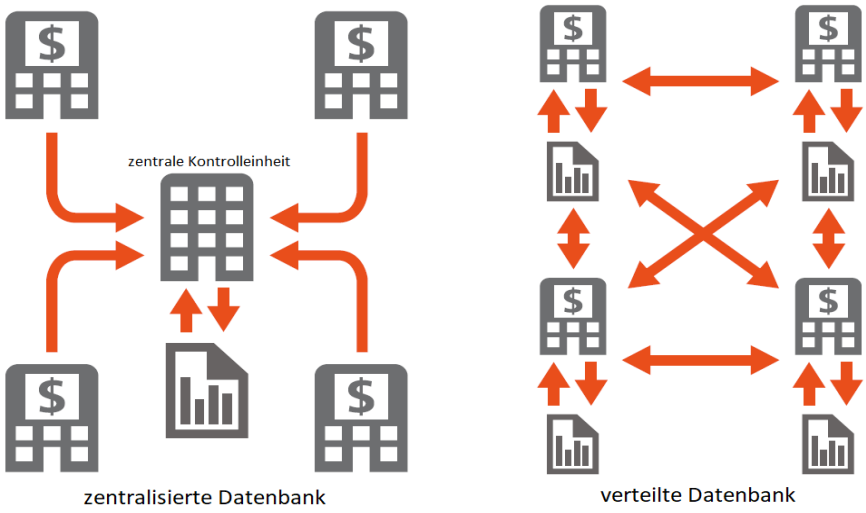

Abbildung 4: Unterschied zentralisierte/verteilte Datenbank
Quelle: In Anlehnung an: DBS Asian Insights; DBS Innovation Group (2016): Understanding Blockchain Technology S. 5. [online]. URL:

---

[26] Vgl. Laurence, Tiana (2018): Blockchain für Dummies S. 26.
[27] Vgl. Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. [online]. URL: https://bitcoin.org/bitcoin.pdf (Abruf: 22.10.2018).
[28] Vgl. Laurence, Tiana (2018): Blockchain für Dummies S.26.

www.dbs.com.sg/treasures/aics/pdfController.page?pdfpath=/content/article/pdf/AIO/AIO_2016/SECTOR-19-001-blockchain-lowres.pdf (Abruf: 18.10.2018).

4.3 Blöcke und Blockchain

Um zu verstehen wie eine Blockchain funktioniert und wie sie sich zusammensetzt, muss der Begriff des „Blockes“ erläutert werden.

Eine betätigte Transaktion wird an das verteilte Peer-to-Peer Netzwerk übermittelt. Dort wird diese, wenn die Transaktion eine korrekte digitale Signatur enthält, von allen full nodes des Netzwerkes aufgenommen und in ihren jeweiligen DL erfasst. Diese aufgenommenen Transaktionen werden, um Speicherplatz zu sparen, in einem sogenannten „Hash-Baum“ gehasht.

Bei einem Hash-Baum wird für alle Transaktionen jeweils ein Hashwert gebildet. Nun werden die Hashwerte in Paare zusammengefügt und aus diesen Paaren werden wiederum Hashwerte gebildet. Dieser Vorgang geht solange weiter, bis ein finaler Hashwert, der sogenannte „Top Hash“ gebildet wird.[29]

Wenn nun eine Transaktion nachträglich manipuliert und geändert werden sollte, würde sich der gesamte Top-Hashwert ändern.

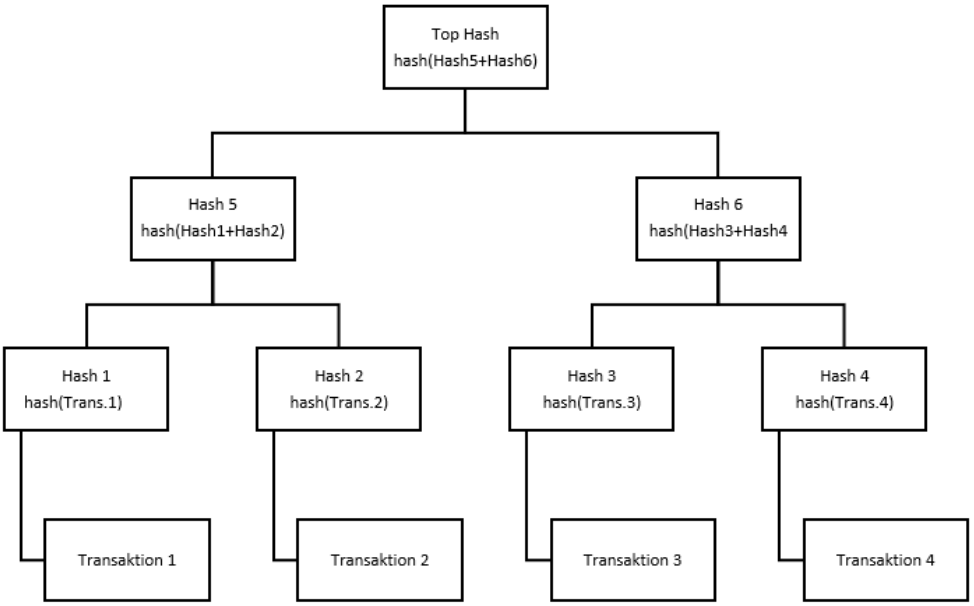

Abbildung 5: Hash-Baum
Quelle: Selbsterstellte Abbildung

[29] Vgl. Narayanan, Arvind u.a. (2016): Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction S. 12 f.

Dieser Top Hash bildet zusammen mit dem vorherigen Header Hash und einem Timestamp einen Block. Im Falle von Bitcoin lag die herkömmliche Blockgröße bei 1 MB.[30] Alle weiteren aufgenommen Transaktionen, die diese Blockgröße überschreiten, werden in den nächsten Block aufgenommen.

Der Timestamp ist ein 4 Byte großer Wert, welcher auf der Anzahl der vergangenen Sekunden, seit dem 1. Januar 1970, basiert.[31]
Für den 1. Januar 2018 (GMT) wäre dieser Wert: „1514764800“.[32]

Der Header Hash ist ein Hashwert, welcher aus dem gesamten Block gebildet wurde. Dadurch, dass ein Block immer den Header Hash des vorherigen Blockes enthält, sind alle Blöcke miteinander verknüpft. Von diesen aneinander geketteten Blöcken stammt der Name Blockchain.[33]

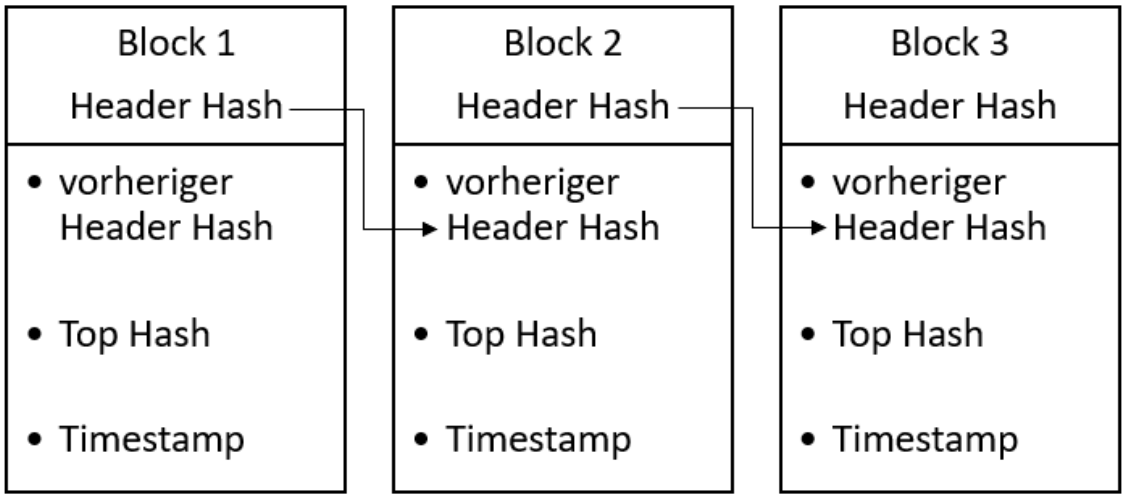

Abbildung 6: Blockchain
Quelle: Selbsterstellte Abbildung

Wenn jemand nun eine Transaktion eines vergangenen Blockes ändern würde, wäre der aktuelle Header Hash des Blockes ungültig. Dieser müsste darauf hin neu berechnet werden. Als Folge dessen, wäre auch der Header Hash der folgenden Blöcke ungültig.

---

[30] Vgl. Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. [online]. URL: https://bitcoin.org/bitcoin.pdf (Abruf: 22.10.2018).
[31] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 37.
[32] Vgl. https://www.epochconverter.com/.
[33] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 38.

Da der erste Block auf keinen vorherigen Header Hash zugreifen kann, wird dieser auch „Genesis Block“ genannt. In den meisten Fällen ist dieser vom Source Code fest vorgegeben.[34]

4.4 Group Consensus

Bis jetzt könnten Transaktionen in der Blockchain ohne großen Aufwand geändert und manipuliert werden. Da jede full node alle Transaktionen notiert und es keine zentrale Kontrolleinheit gibt, ist es schwer eine verbreitete und akzeptierte Wahrheit über den aktuellen Stand des DL zu erreichen. Damit alle full nodes einen gemeinsamen Konsens über den Stand des DL haben, wird ein unmissverständliches Gruppen-Konsens-Verfahren angewendet.[35] Zum aktuellen Zeitpunkt werden zwei verschiedene Verfahren verwendet. Zum einen das Proof of Work Verfahren und zum andern das Proof of Stake Verfahren.[36]

4.4.1 Proof of Work

Wie der Name schon sagt, wird bei der Proof of Work Variante dem DL vertraut, welcher am meisten Rechenarbeit beinhaltet.

Die Rechenarbeit ist in diesem Fall ein bestimmter Wert, welcher dem Block hinzugefügt wird. Dieser Wert wird auch „Nonce“ genannt.

Die Nonce ist ein Wert, welcher generiert wird, um aus dem gesamten Block einen bestimmten Header Hash zu erzeugen. Dieser Header Hash beginnt, je nach Schwierigkeitsgrad, mit einer bestimmten Anzahl an Nullen. Bei der Bitcoin-Blockchain ändert sich dieser Schwierigkeitsgrad alle 2016 Blöcke entweder nach oben oder nach unten. Dies ist abhängig von der Erstellungsdauer der vorherigen 2016 Blöcke.[37]

---

[34] Vgl. Mücke, Thomas (2018): Genesis Block. [online]. URL: https://www.coin-report.net/de/genesis-block/ (Abruf: 18.10.2018).
[35] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology Technology S. 40.
[36] Vgl. Morabito, Vincenzo (2017): Business Innovation Through Blockchain S.10 f.
[37] Vgl. Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. [online]. URL: https://bitcoin.org/bitcoin.pdf (Abruf: 22.10.2018).

In diesem Teil kommt auch die Rechenarbeit ins Spiel. Die einzelnen full nodes versuchen nun, für einen kompletten Block jeweils diese bestimmte Nonce zu finden, damit der Header Hash mit einer bestimmten Anzahl an Nullen beginnt.

Diesen bestimmten Hashwert zu finden ist sehr aufwendig und kann, da es eine Hashfunktion ist, nur durch wiederholtes prüfen zufälliger Werte erreicht werden.

Wenn nun eine full node die passende Nonce gefunden hat, wird der Block inklusive Nonce an das Netzwerk übermittelt. Die anderen Teilnehmer prüfen den Wert und ist dieser korrekt, löschen sie ihren eigenen Block und übernehmen den übermittelten Block.[38]

Wie in Kapitel 4.3 schon erwähnt wurde, sind alle Blöcke miteinander verbunden. Wenn nun jemand eine Transaktion eines vorherigen Blockes ändern würde, müsste diese Person eine neue Nonce für diesen Block und für alle weiteren Blöcke bestimmen. Dies würde einen enormen rechnerischen Aufwand erfordern. Die Blockchain mit der meisten Rechenarbeit ist auch gleichzeitig die längste. Daher bräuchte die Person mindestens 51 % der gesamten Rechenarbeit des Netzwerkes, um die längste Blockchain zu erreichen. Nur so würde sich eine manipulierte Blockchain durchsetzen.

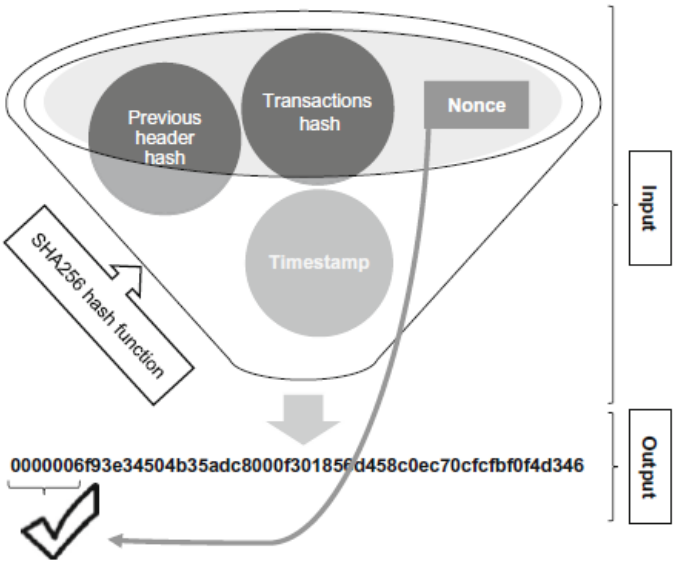

Abbildung 7: Entstehung des Header Hashes
Quelle: Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 41.

[38] Vgl. Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology S. 40 f.

4.4.2 Proof of Stake

Das Proof of Stake Schema ist recht jung und in verschieden Varianten vorhanden. Es ist kostengünstiger, da es nicht wie das Proof of Work Schema enormen Ressourceneinsatz benötigt.

Bei der Proof of Stake Varianten müssen die full nodes keine Rechenarbeit leisten, um Blöcke zu generieren. Die full nodes müssen nur bestimmte Mittel besitzen und diese online halten. Diese Mittel sind so genannte digitale Token der jeweiligen Blockchain und können auch gehandelt werden. Die Wahrscheinlichkeit, dass eine full node einen Block erfolgreich erstellt ist nun abhängig von der Anzahl der Token in ihrem Besitz und nicht von der Rechenleistung. Je höher die Anzahl der Token im Besitz ist, desto höher ist die Wahrscheinlichkeit ausgewählt zu werden, um einen Block zu erstellen.

Um diese Variante zu manipulieren, müsste eine full node im Besitz von über 51% der Token sein. Dies ist jedoch sehr unwahrscheinlich, da der Kauf von 51% aller Tokens hohe Kosten mit sich führen kann.

Ein Vorteil dieser Variante ist eindeutig das Einsparen der Ressourcen für die Rechenleistung. Jedoch besteht die Gefahr der Zentralisierung, indem bestimmte Personen einen Großteil der Token kaufen und besitzen.[39]

[39] Vgl. Morabito, Vincenzo (2017): Business Innovation Through Blockchain S. 11.

5. Supply-Chain-Management

Nachdem die technischen Grundlagen der Blockchain-Technologie erläutert wurden, wird im folgenden Kapitel das SCM als ein mögliches Anwendungsfeld betrachtet, in welchem die Blockchain-Technologie verwendet werden kann. Der Einzelhandelskonzern Walmart verwendet zum Beispiel schon die Blockchain-Technologie, um für die Nahrungssicherheit in seinen Läden zu sorgen.[40]

Das SCM ist ein Bereich mit welchem sich so gut wie jedes Unternehmen beschäftigen muss. Es beinhaltet hohe Kosten und kann auch viele Probleme mit sich bringen. Daher ist es im Interesse von jedem Unternehmen ihr SCM zu verbessern.

Kriterien für ein erfolgreiches SCM gibt es viele. Flexibilität ist eine der wichtigsten Voraussetzungen eines erfolgreichen und effektiven SCM. Flexibilität bedeutet in diesem Fall die Möglichkeit, sich an Strukturwandlungen des Marktes und dessen Produkte anpassen zu können. Es ist von großer Wichtigkeit, dass Unternehmen ohne Verzögerungen auf Nachfrageveränderungen, sowie außerordentliche Ereignisse, reagieren können. Um dies zu erreichen müssen die verschiedenen Teilnehmer der Wertschöpfungskette miteinander kooperieren und Informationen in Echtzeit austauschen. Erst wenn ein reibungsloser Informationsaustausch vorliegt, transparent gearbeitet wird und die Unternehmen sich untereinander vertrauen, kann das SCM erfolgreich sein.[41] In diesem Kapitel wird daher ein genauer Blick auf die Erfolgskriterien Flexibilität, Transparenz, Kooperation und Aktualität der Informationen eines SCM geworfen.

---

[40] Vgl. Galvin, David (2017): IBM and Walmart: Blockchain for Food Safety. [online]. URL: https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf (Abruf: 09.10.2018).

[41] Vgl. Kopecka, Jarmila; Penner, Guido; Santema, Sicco (2002): Flexibility in supply chain managment S. 2 f. [online]. URL: https://www.impgroup.org/uploads/papers/7315.pdf (Abruf: 17.10.2018).

5.1 Probleme des SCM

Bevor dargestellt wird wie ein Unternehmen die Blockchain-Technologie implementieren kann, ist es zunächst wichtig, verschiedene ausgewählte Probleme des SCM aufzuführen.

Bei dem SCM fallen regelmäßig unvorhersehbare Ereignisse an, welche sich negativ auf das Unternehmen auswirken. Um am kosteneffektivsten zu arbeiten und alle Teilnehmer der Wertschöpfungskette zufrieden zu stellen, sollten solche unvorhersehbaren negativen Auswirkungen reduziert werden.

5.1.1 Globalisierung

Die zunehmende Globalisierung ist Ursache zahlreicher Probleme. Viele Unternehmen produzieren und verarbeiten ihre Produkte aus Kostengründen nicht mehr im eigenen Land, sondern outsourcen ihre Produktion. Oftmals nicht nur in ein bestimmtes Land, sondern in mehrere Länder der Welt. Deshalb müssen die verschiedenen Produktionsanlagen aufeinander abgestimmt werden. Sie müssen beispielsweise hinsichtlich der Produktion, der Lagerung und des Transportes koordiniert werden und miteinander kooperieren. Unternehmen können oftmals, als Folge dessen, ihre zeitlichen Vorgaben nicht einhalten und es kommt vermehrt zu Produktionsausfällen.

5.1.2 Echtzeit-Informationsstand

Viele Unternehmen haben das Problem nicht immer den aktuellen Informationsstand der gesamten Wertschöpfungskette zu kennen. Stets zu wissen, welche Menge nachgefragt wird, welche Lieferung sich wo befindet und ob es zu Verzögerungen kommt, bringt erhebliche Vorteile mit sich. Die Kenntnis des „Echtzeit-Informationsstandes“ erlaubt einem Unternehmen auf das Eintreten von Verzögerungen oder auf erhöhte Nachfrage effektiver und schneller zu reagieren. Stets auf dem aktuellsten Informationsstand zu sein, ermöglicht auch einen permanenten Überblick über das aktuelle Inventar. Versandte Güter können auf ihrem Weg zum Adressaten genau verfolgt werden. Dadurch könnten „out of stock“ Situationen vermieden werden oder schon versandte Güter zu den benötigten Stellen

umgelenkt werden. Auch der Kunde wäre immer auf dem aktuellsten Stand und das Unternehmen kann transparenter arbeiten und so Vertrauen aufbauen. Um einen solchen, stets aktuellen Informationsstand zu erreichen, müssen jedoch alle Unternehmen einen erhöhten Aufwand betreiben und den anderen Unternehmen vertrauen.

5.1.2.1 Ripple-Effekt

Der Ripple-Effekt, auch Schneeball-Effekt genannt, beschreibt, dass kleine Störungen an einer beliebigen Stelle der Wertschöpfungskette erhebliche Auswirkungen auf die gesamte Kette haben können.

Wenn es zum Beispiel an einer Stelle der Wertschöpfungskette Lieferprobleme oder Störungen gibt, wird die nachgeordnete Stelle nicht wie geplant beliefert und hat daher auch Probleme. Dieser Effekt entwickelt sich die gesamte Wertschöpfungskette entlang.

Gründe für diesen Effekt sind leicht zu lokalisieren. So sind viele Unternehmen durch die Globalisierung abhängig von einem konstanten Transport von Gütern und einer dafür bestehenden Infrastruktur. Wenn Unternehmen nur einen Lieferanten besitzen und dieser Probleme bei der Lieferung hat, kann das Unternehmen nicht so leicht die Produkte von einem anderen Lieferanten beziehen. Das Unternehmen ist auf seinen Notfallbestand angewiesen und wenn dieser zu Neige geht, liegt eine out-of-stock Situation vor. Durch die fehlende Transparenz entlang der Wertschöpfungskette besteht nicht die Möglichkeit, schnell genug auf auftretende Probleme zu reagieren.[42]

5.1.2.2 Bullwhip-Effekt

Der Bullwhip-Effekt ist ein lang bekanntes Phänomen, bei welchem es Abstimmungs- und Kommunikationsprobleme entlang der Supply-Chain gibt. Bei einer ungeplanten Steigerung der Nachfrage von beispielsweise 10% erhöhen die Hersteller ihre Produktion um bis zu 40%. Diese erhöhte Produktion entsteht durch nicht

[42] Vgl. Ivanov, Dmitry (2018): Structural Dynamics and Resilience in Supply Chain Risk Management S. 34 ff.

vorhandenes Wissen der aktuellen Nachfrage. Bei einer Erhöhung der Endkundennachfrage, passen vorgelagerte Stufen ihre Bestellmengen und Produktion an. Die nächste Stufe ist einer höheren Bestellmenge ausgesetzt und erhöht die eigene Bestellmenge daher noch mehr. Dieser Effekt zieht sich bis zur letzten Stelle der Wertschöpfungskette durch. Diese Schwankungen, sollen sich erst nach gut einem Jahr auf die 10% Steigerung anpassen. Als Folge dessen haben Unternehmen einen erhöhten Lagerbestand, welcher zusätzliche Kosten verursacht.

Es gibt mehrere Ursachen für diesen Effekt. Zum einen sind keine zentralen, sondern nur lokale Informationen verfügbar. Jede Stufe der Wertschöpfungskette erhält nur Informationen von der vorherigen und nachfolgenden Stufe. Des Weiteren kommen Zeitverzögerungen in der Bearbeitung und eine Bündelung von Aufträgen dazu. Dadurch ist die Endkundenachfrage in der Lieferkette nicht mehr deutlich zu erkennen. [43, 44]

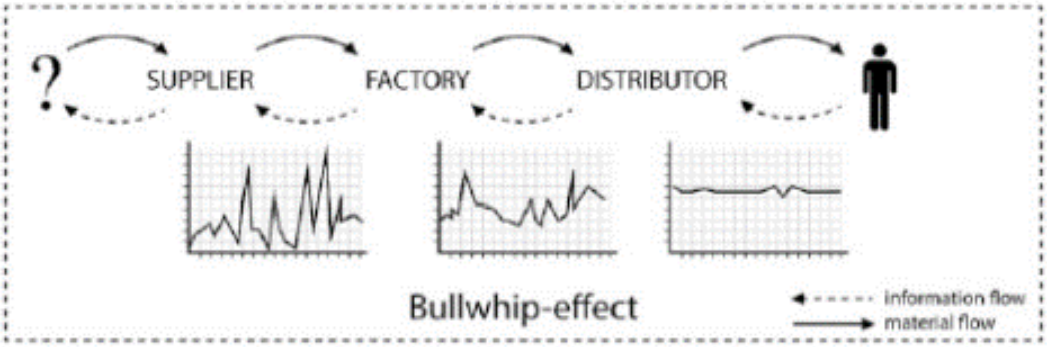

Abbildung 8: Bullwhip-Effekt
Quelle: Ivanov, Dimitry (2018): Structural Dynamics and Resilience in Supply Chain Risk Management S.31.

[43] Vgl. Werner, Hartmut (2017): Supply Chain Management Grundlagen, Strategien, Instrumente und Controlling S. 47 f.
[44] Vgl. Ivanov, Dmitry (2018): Structural Dynamics and Resilience in Supply Chain Risk Management S. 31.

5.1.3 Compliance und Qualität

Laut Umfragen legen die deutschen Bürger immer mehr Wert auf Qualität alltäglicher Produkte.[45] Daher ist es wichtig, dass Unternehmen qualitativ hochwertige Produkte erzeugen. Dies fängt schon in den ersten Stufen der Wertschöpfungskette an, wie zum Beispiel der Auswahl der verwendeten Rohmaterialien.

Compliance ist ein weiterer Punkt, welcher mit der Qualität der Produkte einhergeht. So müssen die Unternehmen dafür sorgen, dass die Produkte bestimmte Standards einhalten. Daher muss jeder Teil der Wertschöpfungskette bestimmte Qualitätsstandards einhalten. Unternehmen müssen dazu Compliance-Dokumente wie Lizenzen und Zertifikate dokumentieren. Die Dokumentationen bedeuten einen hohen Arbeitsaufwand für das Unternehmen.

5.1.4 Vertrauen

Zwischen verschiedenen Unternehmen gibt es schon seit jeher Vertrauensprobleme. Wenn kein Vertrauen zwischen Unternehmen besteht, wird nicht optimal gearbeitet. Es wird alles doppelt inspiziert und Zertifikate verifiziert.[46] Dazu besteht die Sorge, dass zu Verfügung gestellte Informationen an potentielle Konkurrenten weitergegeben werden. Als Ergebnis dessen wird selbst den geteilten Informationen nicht vollständig vertraut.[47]

---

[45] Vgl. Primärquelle von de.statista.com (2016): Bevölkerung in Deutschland nach Einstellung zur Aussage „Ich bin auch bei Produkten des täglichen Lebens sehr anspruchsvoll“ von 2013 bis 2016 (in Millionen). [online] URL: https://de.statista.com/statistik/daten/studie/172161/umfrage/einstellung-hoher-anspruch-auch-bei-alltaeglichen-produkten/ (Abruf: 09.10.2018).

[46] Vgl. G. Kwon, Ik-Whan; Suh, Taewon (2006): Facotrs Affecting the Level of Trust and Commitment in Supply Chain Realtionships. [online]. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-493X.2004.tb00165.x (Abruf: 09.10.2018).

[47] Vgl. IBM Institute for Business Value (2016): Trust in trade Toward stronger supply chains. [online]. URL: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN (Abruf: 09.10.2018).

5.2 Blockchain-Technologie im SCM

Wie genau kann die Blockchain-Technologie helfen diese Probleme des SCM zu beheben und generell das SCM zu verbessern? In diesem Abschnitt werden Ansätze betrachtet, wie die Blockchain-Technologie das SCM revolutionieren kann. Die Implementierung und die Vorteile werden anhand einer Lebensmittel Wertschöpfungskette dargestellt.

Zunächst muss betrachtet werden, wie die Blockchain-Technologie sich in ein SCM-System integrieren lässt. Dazu kann ein Blockchain-Konstrukt für das SCM erstellt werden, welches aus vier verschiedenen Ebenen besteht, einmal der IOT-Ebene, dann der Blockchain-Ebene, darauf folgt die Smart Contract-Ebene und als letztes die Unternehmensebene.[48]

Nachdem jede Ebene erläutert wurde, wird an einem Beispiel dargestellt, wie wichtig die Blockchain-Technologie für das SCM sein kann.

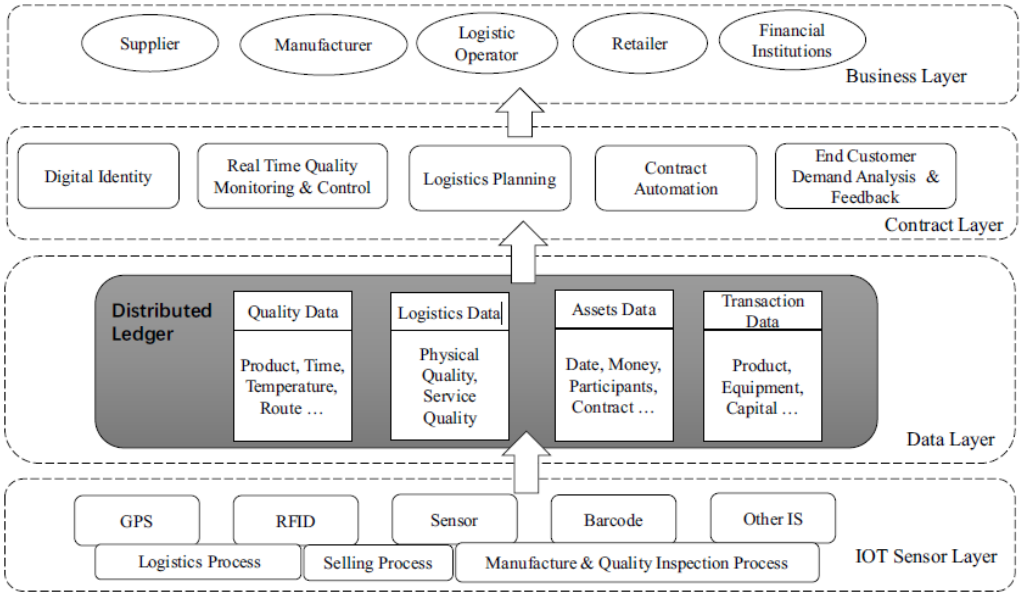

Abbildung 9: SCM Blockchain Konstrukt
Quelle: Chen, Si u.a. (2017): A Blockchain-Based Supply Chain Quality Management Framework S.2. [online]. URL: https://www.researchgate.net/publication/321027278_A_Blockchain-Based_Supply_Chain_Quality_Management_Framework (Abruf: 10.10.2018).

[48] Vgl. Chen, Si u.a. (2017): A Blockchain-Based Supply Chain Quality Management Framework S.2. [online]. URL: https://www.researchgate.net/publication/321027278_A_Blockchain-Based_Supply_Chain_Quality_Management_Framework (Abruf: 10.10.2018).

5.2.1 IOT-Ebene

Die erste Ebene ist die IOT-Ebene. Diese Ebene befasst sich mit der gesamten Aufnahme von Informationen. Dafür werden Güter mit RFID-Chips, Barcodes und in bestimmten Fällen auch mit einem GPS versehen. Ein GPS ermöglicht die Güter konstant zu lokalisieren. Die RFID-Chips oder Barcodes sind dazu da, um Informationen über das Produkt aufzunehmen. Diese beinhalten, um was für ein Produkt es sich handelt, Informationen zu der Qualität des Produktes, wer es gehandhabt hat, welche Qualitätskontrollen durchgeführt wurden und wann es wo war. Des Weiteren können Güter auch noch mit Sensoren versehen werden, welche Daten aus der realen Welt, wie beispielsweise Temperatur oder Luftfeuchtigkeit, aufnehmen.

Diese Sensoren spielen beispielsweise eine große Rolle für die Sicherheit von Nahrungsmitteln. So kann ein gefangener Fisch in der Nordsee direkt mit einem Sensor versehen werden, welcher stets die Temperatur misst und aufzeichnet. Wenn dieser Fisch nun bis nach Japan transportiert werden sollte, um dort zu Sushi verarbeitet zu werden, besteht die Möglichkeit zu überprüfen, ob die Kühlkette nicht unterbrochen wurde.

In der heutigen Zeit ist die Verwendung von RFID-Technologie oder einfachen Barcodes nichts Neues oder Besonderes. Sie sind erforderlich um die gesamten aufgenommenen Informationen an die zweite Ebene, die zuständige Blockchain, zu übermitteln, in welcher jegliche Informationen gespeichert werden.

Des Weiteren können Dokumente, Zertifikate und andere Papiere an die Blockchain übermittelt werden.

Der Transport von Gütern geht mit einer hohen Menge an Papierdokumenten einher. Diese Dokumente werden oft nicht digitalisiert und müssen deshalb auf herkömmliche Wege (meist per Post) versendet und übermittelt werden. Dokumente über die Verwendung von Chemikalien, Pestiziden oder über die Qualität des Produktes müssen von den jeweiligen Unternehmen erstellt werden und dann jeweils auf herkömmliche Weise zum Ziel gebracht werden, da eingescannte Kopien nicht das volle Vertrauen genießen. Der kleinste Fehler, wie zum Beispiel eine unvollständige Anschrift, kann hier zu mehreren Tagen Verspätung führen, was sich

nach dem im Kapitel 5.1.2.2 erklärten Rippel-Effekt auf die gesamte Versorgungskette auswirken kann. Daher ist es im Interesse aller Teilnehmer auch diese Dokumente zu digitalisieren, um so Zeitverzögerungen zu vermeiden. Die Blockchain-Technologie bietet die Möglichkeit Dokumente, welchen sonst nur im Originalem vertraut wird, fälschungssicher digital zu übermitteln. Dies ist möglich, da jeder Teilnehmer eine einzigartige, eigene digitale Signatur besitzt und sich die Teilnehmer dadurch sicher sein können, dass die verfügbaren Informationen von dem richtigen Absender kommen. Bei der Blockchain-Technologie sind eingetragene Informationen nicht mehr veränderbar. Daher können vorhandene Dokumente nicht mehr nachträglich geändert oder manipuliert werden.

In der folgenden Abbildung ist gut zu erkennen, wie viele verschiedene Stellen Daten an die Blockchain senden und welche Informationen das beispielsweise sein können. Diese Darstellung spiegelt jedoch nicht den gesamten Prozess des SCM mit Hilfe einer Blockchain wieder. In den folgenden Kapiteln wird diese noch vervollständigt.

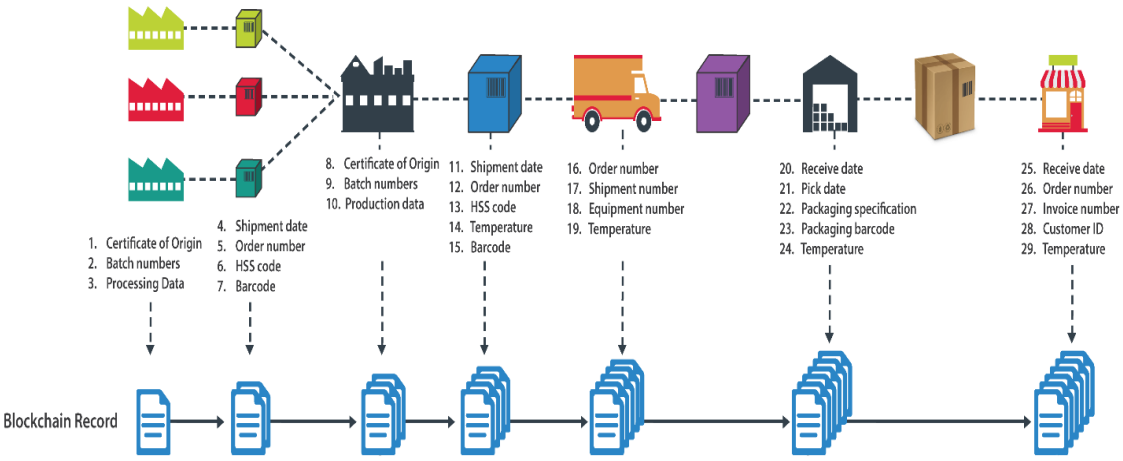

Abbildung 10: IOT-Ebene
Quelle: Online im Internet: Mullaney, Ryan (2018): Blockchain becomes a crucial link in the supply chain. URL: https://aqurus.ca/blockchain-crucial-link-supply-chain/ [Ausschnitt] (Abruf: 25.10.2018).

Somit legt die IOT-Ebene den Grundstein, um konstante Echtzeit-Verfolgung zu ermöglichen und die Qualität der Produkte zu kontrollieren. Einige zurzeit bestehende Probleme können so behoben werden. Wie genau dies möglich ist, wird in dem nächsten Abschnitt erläutert.

5.2.2 Blockchain-Ebene

Die zweite Ebene ist die Blockchain-Ebene, welche das Herz des gesamten Konstrukts ist. In ihr werden die gesamten Informationen aus der IOT-Ebene aufgenommenen und eingetragenen.

Dies geschieht, indem die verschiedenen Informationen in Blöcke aufgenommen werden, welche dann miteinander verknüpft werden. Da die Blockchain ein dezentrales und verteiltes System ist, müssen sich alle Teilnehmer auf eine Wahrheit des Standes der Blockchain einigen. Dies geschieht über einen ausgewählten Group Consensus. Dadurch haben alle Teilnehmer der Blockchain, ob groß oder klein, das gleiche Stimmenrecht und es wird keiner bevorzugt. Dieser Stand der Blockchain wird dann generell akzeptiert und ist nicht mehr änderbar.

5.2.2.1 Transparenz der Blockchain

Ein großer Vorteil der Blockchain-Technologie ist das Ermöglichen von kompletter Transparenz entlang der Wertschöpfungskette. Auf die in der Blockchain eingetragenen Informationen können, je nachdem ob es eine private- oder öffentliche Blockchain ist, jeder oder nur ausgewählte Personengruppen stets zugreifen.

Der unbeschränkte Zugriff auf die eingetragenen Informationen hilft erheblich dabei, Probleme, welche durch Globalisierung auftreten und allgemeine Echtzeit-Informationsprobleme, zu beseitigen. Unternehmen haben jetzt erstmals jederzeit Zugriff auf nicht manipulierbare Informationen, ohne dafür auf ein weiteres Unternehmen angewiesen zu sein.

Durch die stets aktuellen Informationen können Fragen, wie ob die Ware schon versendet wurde, wer sie zurzeit handhabt oder ob das Schiff den Hafen zur richtigen Zeit verlassen hat, direkt beantwortet werden. Dazu muss nicht mehr mehrere Tage auf einen Brief gewartet werden oder zahlreiche Anrufe getätigt werden, was Zeit und Nerven kostet. Ein Unternehmen kann nämlich in nur wenigen Sekunden alle Informationen in der Blockchain einsehen.

Wenn Probleme wie der Bullwhip- oder Ripple-Effekt betrachtet werden, entstehen diese durch unzureichende Kommunikation und fehlender Transparenz entlang der Wertschöpfungskette. Unternehmen können mithilfe der Blockchain-Technologie direkt erkennen, wie viele Produkte produziert, angefordert und verkauft werden. Anhand dieser Daten können sie Ihre eigene Produktion, ihre Bestellungen oder ihr Inventar anpassen. Wenn es in einem Teil der Wertschöpfungskette zu Problemen kommt und Güter nicht rechtzeitig geliefert werden können, ist dies für alle Teilnehmer direkt sichtbar. So können sie Gegenmaßnahmen einleiten, um selbst keine negativen Auswirkungen von den Problemen zu erfahren. Komplette Transparenz der Wertschöpfungskette ermöglicht auch Just-in-time-Produktion zu optimieren. Lieferungen können genauer aufeinander abgestimmt werden und es kann bei Verspätungen direkt reagiert werden. Dadurch, dass alle Teilnehmer auf Änderungen und unerwartete Ereignisse direkt reagieren können, werden Schwankungen in der Produktion und Bestellung vermieden und so das Inventar immer auf dem optimalen Stand gehalten.

Ein weiterer Vorteil ist, dass die Historie der Blockchain nicht mehr änderbar ist. Dadurch werden Manipulations- und Vertuschungsversuche verhindert. Unternehmen können Fehler, welche sie begangen haben, nicht mehr verheimlichen, da sie für immer einsehbar und nicht veränderbar sind. Diese unveränderbaren und transparenten Informationen lösen auch Streitigkeiten zwischen Unternehmen auf. Wenn es beispielsweise zu einem Konflikt zwischen zwei Unternehmen über eine zu späte und beschädigte Lieferung kommt, kann geprüft werden, wer die Ware zuletzt gehandhabt hat, in welcher Verfassung sie zu diesem Zeitpunkt war und wann sie versendet wurde. Jeder Teilnehmer hat den Zugriff auf den gleichen Stand der Blockchain, wodurch Meinungsverschiedenheiten nicht entstehen können.

5.2.2.2 Vertrauen

Vertrauen zwischen Unternehmen aber auch zwischen Unternehmen und Konsumenten ist ein wichtiger Erfolgsfaktor. So ist es vielen Konsumenten immer

wichtiger, Bio oder Fair-Trade Produkte zu konsumieren.[49, 50] Jedoch gibt es in diesem Gebiet eine große Vertrauenslücke. Konsumenten sind oft unsicher, ob das vorliegende Produkt wirklich Bio oder wirklich aus fair gehandelter Produktion stammt. Um diese Unsicherheiten zu beheben können auch Konsumenten von der Transparenz der Wertschöpfungskette profitieren. So können sie den Barcode oder RFID-Chip des Produktes mithilfe eines Handys oder einem vor Ort bereitgestellten Gerät einscannen und so eine komplette Übersicht über das Produkt erhalten. Die Konsumenten können direkt im Supermarkt erkennen, wie das Produkt behandelt wurde, woher es kommt und unter welchen Bedingungen gearbeitet wurde. Unternehmen wären dadurch in der Lage, Vertrauen zu ihren Kunden aufzubauen und Misstrauen zu beseitigen.

Die Blockchain-Technologie hilft auch dabei, zwischen Unternehmen das bisher so schwierige aber benötigte Vertrauen aufzubauen. Dafür wird die gesamte Aufzeichnung aller bisheriger Transaktionen als Grundlage verwendet. Anhand dieser lässt sich genau zurückverfolgen, wie ein Unternehmen bisher gearbeitet hat, ob es seine Zeitfenster eingehalten hat und ob es jemals zu Problemen kam. Dadurch ist ein Unternehmen schon fast gezwungen, ohne Fehler und ordnungsgemäß zu arbeiten, da sonst potentielle neue Kunden nicht angeworben werden können. Unternehmen können den weitergegebenen Informationen vertrauen und müssen nicht alle Unterlagen doppelt kontrollieren. Zertifikate und weitere Dokumente können direkt eingesehen werden. Anhand der digitalen Signatur jedes Teilnehmers lassen sich die Dokumente auch unmittelbar dem Ersteller zuordnen, so lässt sich die Legitimität eines Dokumentes beweisen.

---

[49] Vgl. Primärquelle von de.statista.com (2018): Umsatz mit Bio-Lebensmitteln weltweit in den Jahren 1999 bis 2016 (in Milliarden US-Dollar). [online] URL: https://de.statista.com/statistik/daten/studie/187590/umfrage/weltweiter-umsatz-mit-bio-lebensmitteln-seit-1999/ (Abruf: 09.10.2018).

[50] Vgl. Primärquelle von de.statista.com (2017): Umsatz mit Fairtrade-Produkten weltweit in den Jahren 2004 bis 2016 (in Millionen Euro). [online]. URL: https://de.statista.com/statistik/daten/studie/171401/umfrage/umsatz-mit-fairtrade-produkten-weltweit-seit-2004/ (Abruf: 09.10.2018).

5.2.2.3 Betrug

Fälschungen und Betrüger gibt es überall auf der Welt. Sie schaden unwissenden Konsumenten und auch den originalen Herstellern. Die Europäische Kommission ging davon aus, dass im Jahr 2005 durch Fälschungen und Plagiate ein jährlicher volkswirtschaftlicher Schaden von 200 bis 300 Milliarden Euro entstand und dazu noch über 200.000 Arbeitsplätze vernichtet wurden.[51] Daher ist es wichtig, den Kunden die Möglichkeit zu geben, Fälschungen direkt zu identifizieren und so den Umlauf von gefälschten Produkten zu verringern.

Im Bereich der Arzneimittel wäre dies ein wichtiger Fortschritt. Die World Health Orgranization geht davon aus, dass 10% der Arzneimittel in Entwicklungsländern Fälschungen sind.[52] Gerade bei Arzneimittel ist der Umgang mit Fälschungen ein ernstes Thema, da viele Leben von einer richtigen Behandlung abhängig sind.

Mit Hilfe der Blockchain-Technologie bekommen die Käufer die Möglichkeit, die vorliegende Ware direkt zu überprüfen. Die Produkte werden bei der Herstellung schon in die offizielle Blockchain der Hersteller eingetragen. So muss der Käufer nur den Barcode oder den RFID-Chip mit seinem Handy oder einem anderen Gerät einscannen und bekommt sofort die Information, ob es sich bei dem Produkt um ein Original handelt. Dieses Verfahren kann sich für eine Vielzahl von Produkten eignen. So kann auch die Herkunft von Diamanten verfolgt werden, um so die Anzahl der sogenannten Blutdiamanten zu verringern. Aber auch Luxusgüter wie Uhren und Handtaschen können so verifiziert werden.

---

[51] Vgl. IHK-Wirtschaft in Mittelfranken (2005): Welche Folgen hat die Produktpiraterie?. [online]. URL: https://www.ihk-nuernberg.de/de/IHK-Magazin-WiM/WiM-Archiv/WIM-Daten/2005-12/Wirtschaftsfragen/Welche-Folgen-hat-die-Produktpiraterie-.jsp (Abruf: 09.10.2018).

[52] Vgl. World Health Organization (2017): 1 in 10 medical products in developing countries is substandard or falsified. [online] URL: http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified (Abruf: 09.10.2018).

5.2.3 Smart Contract-Ebene

Die dritte Ebene ist die Smart Contract Ebene. Smart Contract ist vielen noch ein fremder Begriff, jedoch können sie das Leben wie wir es kennen grundlegen verändern.

Smart Contracts sind im Grunde programmierbare Verträge, welche sich automatisch ausführen, wenn die vorgegebenen Bestimmungen erreicht sind.[53] Die Anwendungsmöglichkeiten von Smart Contracts erstrecken sich jedoch viel weiter. Smart Contracts lassen sich besser als ausführbare Programme auf Grundlage der Blockchain beschreiben. Der simpelste Smart Contract bei dem Beispiel des SCM wäre die Bezahlung eines gelieferten Produktes. So würde der Smart Contract, welcher die Bezahlung eines Produktes beinhält, ausgeführt werden, wenn das Produkt ordnungsgemäß geliefert wurde.

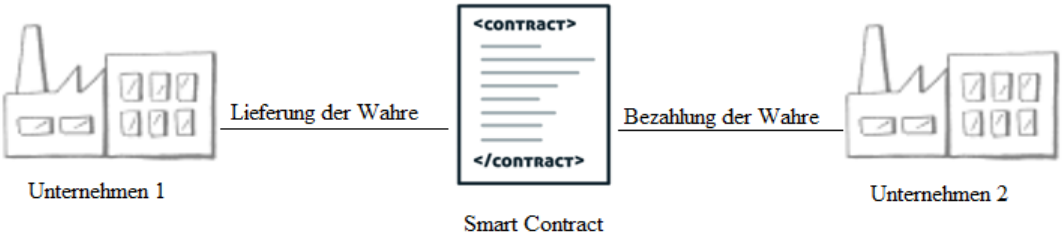

Abbildung 11: Beispiel Smart Contract
Quelle: Selbsterstellte Abbildung

Die gesamten gesammelten Daten aus den Ebenen davor dienen als Grundlage für Smart Contracts. Auf diese können Smart Contracts selbstständig zugreifen und so die Effizienz der Wertschöpfungskette verbessern. So können Smart Contracts nicht nur für Verträge verwendet werden, sondern logistische Aufgaben auch selbstständig planen.

Aufgaben in denen Smart Contracts verwendet werden können sind:

- Kundennachfrage berechnen
- Produktion und Bestellungen optimieren
- Angekommene Produkte bezahlen
- Inventar anpassen

[53] Vgl. Cant, Bart u.a. (2017): Smart Contracts in Financial Services: Getting from Hype to Realtiy. [online]. URL: https://www.capgemini.com/wp-content/uploads/2017/07/smart_contracts_in_fs.pdf (Abruf: 09.10.2018).

- ❖ Verschiedene Produktionsstandpunkte/Lieferanten aufeinander abstimmen
- ❖ Qualität und Zertifikate prüfen

Die oben aufgelisteten Punkte sind nur ein paar wenige Beispiele. Smart Contracts haben das Potential bei so gut wie jeder Aufgabe das Unternehmen zu unterstützen und Prozesse zu automatisieren. Die Darstellung aus Kapitel 5.2.1 kann nun vervollständigt werden.

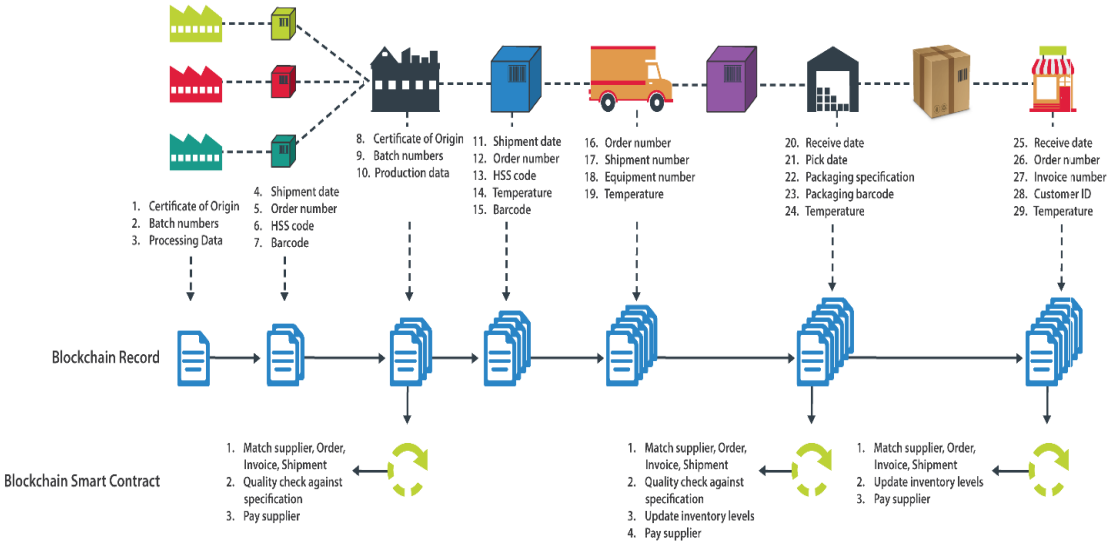

Abbildung 12: Zusammenspiel der drei Ebenen
Quelle: Online im Internet: Mullaney, Ryan (2018): Blockchain becomes a crucial link in the supply chain. URL: https://aqurus.ca/blockchain-crucial-link-supply-chain/ (Abruf:25.10.2018).

Durch die Kombination von der totalen Transparenz der Blockchain und die Automatisierung der Smart Contracts werden viele der zurzeit bestehenden Probleme gelöst. Probleme, die durch den Bullwhip- oder Ripple-Effekt verursacht wurden, werden nicht mehr zu Stande kommen. Die Smart Contracts passen die Bestellungen und die Produktion an den genauen Bedarf an, welcher durch die Informationen aller Stellen der Wertschöpfungskette bestimmt wurde. Dadurch ist das Inventar immer auf optimalen Stand.

Just-in-time-Produktion kann dadurch auch optimiert werden, da Smart Contracts das Unternehmen bei der optimalen Planung mit den vorliegenden Informationen unterstützen kann.

Smart Contracts stellen sicher, dass für eine erbrachte Leistung auch der abgemachte Betrag bezahlt wird. Unternehmen müssten nicht mehr die Sorge haben, verspätete oder gar keine Zahlung für ihre Dienste zu erhalten.

5.2.4 Unternehmens-Ebene

Die letzte Ebene ist die Unternehmens-Ebene. Ganz von selbst kann das SCM eines Unternehmens noch nicht ablaufen.

Smart Contracts nehmen ihre Informationen aus der Blockchain, welche nur vergangene Daten enthält. Daraus lassen sich einige Prognosen erstellen und Empfehlungen anfertigen, zukünftige Ereignisse werden jedoch nicht beachtet. Auch außerordentliche Ereignisse wie Umweltkatastrophen oder Epidemien lassen sich nicht vorhersagen oder aus vergangenen Daten berechnen.

Daher können sich die Unternehmen nicht rein auf Vorgaben aus Smart Contracts verlassen. Die beispielsweise berechneten Kauf- und Herstellungsvorschläge von Smart Contracts dienen für ein Unternehmen nur als Vorlage. Es muss entschieden werden, ob die Vorschläge ausgeführt werden oder ob etwas geändert werden muss.[54]

[54] Vgl. Chen, Si u.a. (2017): A Blockchain-Based Supply Chain Quality Management Framework S. 1 f. [online]. URL: https://www.researchgate.net/publication/321027278_A_Blockchain-Based_Supply_Chain_Quality_Management_Framework (Abruf: 10.10.2018).

5.3 Anwendungsbeispiel E. coli

Im September 2006 fand in Nordamerika ein Ausbruch des Escherichia coli Bakterium (auch E. coli genannt) statt. Es wurden 205 Personen infiziert, wovon 3 verstarben. Nach einigen DNA-Tests fanden die Labore am 13. September 2006 heraus, dass sich alle Patienten mit dem gleichen Bakterienstamm infiziert hatten. Dieses Bakterium befand sich in frischem Spinat. Als Folge ordnete die U.S Food and Drug Administration an, dass alle Spinatprodukte aus den Supermärkten entfernt werden sollten und es wurde ein landesweiter Aufruf gemacht, keinen Spinat mehr zu konsumieren. Am 20. September 2006 konnte ein bestimmtes Produkt identifiziert werden, welches mit diesen Bakterien kontaminiert war. Es stellte sich auch heraus, dass das infizierte Produkt noch in weitere Länder exportiert wurde. Da es nicht möglich war, das Produkt in den anderen Ländern zu verfolgen, musste das gesamte Lebensmittelnetzwerk in den betroffenen Ländern informiert werden. Erst am 29. September 2006, also nach neun Tagen, konnte der Ursprung des Produktes, einer einzigen Farm in Kalifornien, zugeordnet werden. In diesem gesamten Zeitraum wurde kein Spinat verkauft. Das hatte neben den erkrankten Menschen auch für die Farmer weitreichende Folgen. Die gesamte Spinaternte durfte nicht verkauft werden und wurde vernichtet. Dadurch hatten viele Farmer existenzielle Probleme und litten unter erheblichen finanziellen Einbußen.[55, 56]

Wäre die Blockchain-Technologie schon damals im SCM implementiert gewesen, hätte sich dieser Vorfall komplett anders entwickelt.

Bis der Spinat den Konsumenten zu Verfügung steht, durchläuft er einige Prozesse und legt einen weiten Weg zurück. Sein Weg beginnt bei einem Bauern auf dem Feld und endet in einem Supermarkt im Regal. Dazwischen wird er verarbeitet, gelagert und mehrmals transportiert. Bei jeder dieser Stationen der Wertschöpfungskette werden Informationen in die Blockchain eingetragen. Um zu verstehen, wie sich die

---

[55] Vgl. The Food Industry Center, University of Minnesota; National Center for Food Protection and Defense (2009): Natural Selection: 2006 E. coli Recall of Fresh Spinach A Case Study by The Food Industry Center. [online]. URL: http://ageconsearch.umn.edu/bitstream/54784/2/Natural%20Selection.pdf (Abruf: 09.10.2018).

[56] Vgl. World Health Organization; International Food Safety Authorities Network (2007): Escherichia coli O157:H7 outbreak in spinach. [online]. URL: http://www.who.int/foodsafety/fs_management/No_01_spinach_Feb06_en.pdf (Abruf: 09.10.2018).

Blockchain-Technologie in diesem Beispiel positiv ausgewirkt hätte, muss zunächst der gesamte Weg des Spinates dargestellt werden.

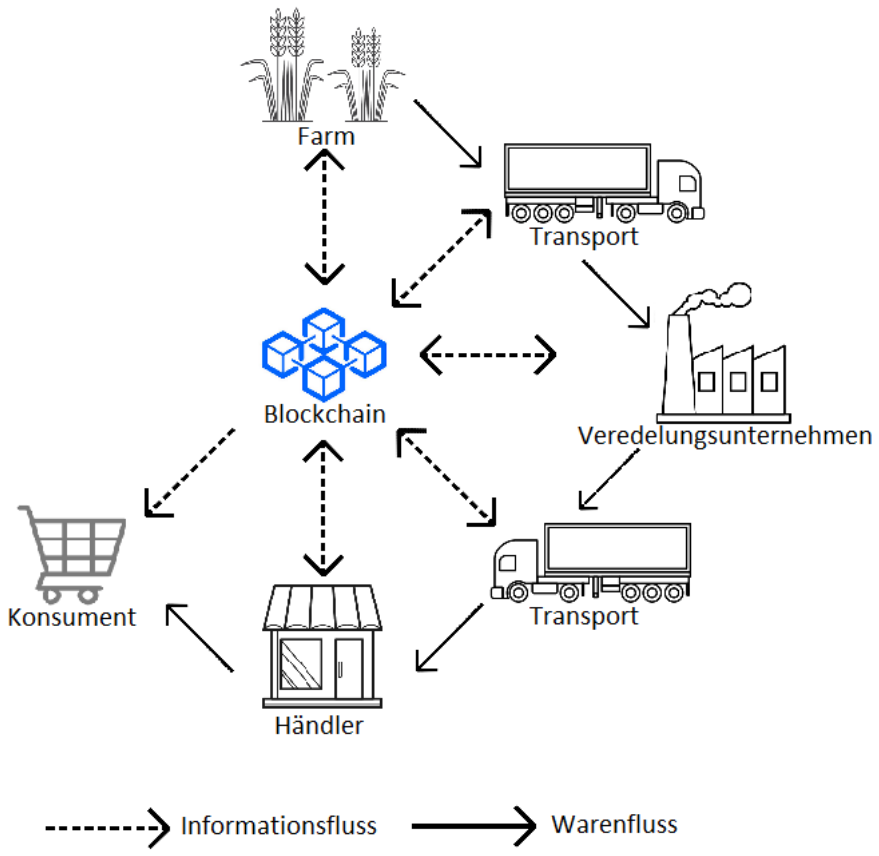

Abbildung 13: Der Weg des Spinates
Quelle: Selbsterstellte Abbildung. Verwendete Vektorgrafiken: https://www.vecteezy.com.

Zu Beginn pflanzt und erntet der Bauer den Spinat. Dabei trägt er in die Blockchain ein um welche Art es sich handelt, welche Chemikalien verwendet wurden und wo der Spinat gezüchtet wurde. Nach der Ernte wird der Spinat zu einem Veredelungsbetrieb transportiert. Bei dem Transport werden Abfahrzeit und -ort an die Blockchain übermittelt. Während des gesamten Transportes nehmen Sensoren Temperatur und Luftfeuchtigkeit auf, um so die Qualität des Spinates zu sichern. Das Veredelungsunternehmen kann genau erkennen, wann der Transporter losgefahren ist und Smart Contracts helfen ihm dabei, die Ankunft weiterer Lieferungen zu planen, um einen Lieferstau zu vermeiden. Wenn der Spinat beim Veredelungsbetrieb angekommen ist, wird dies an die Blockchain übermittelt. Die Ware wird mit Hilfe von Smart Contracts geprüft und automatisch bezahlt. Der Spinat wird veredelt und die neuen Produkte werden in die Blockchain eingetragen. Smart Contracts aktualisieren das Inventar und planen neue Lieferungen und Bestellungen. Bis der veredelte Spinat an Händler weitertransportiert wird, muss er unter genau

definierten Bedingungen gelagert werden. Auch hier helfen Sensoren, welche Temperatur und Luftfeuchtigkeit überwachen.

Können die vorgegebenen Werte zu irgendeinem Zeitpunkt nicht eingehalten werden, muss das Produkt aus dem Verkehr genommen werden. Ein Fehler, wie zum Beispiel die Unterbrechung der Kühlkette, kann nicht verheimlicht werden, da diese Information sich für immer in der Blockchain befinden. Der potentielle Käufer sieht es sofort und wird so geschützt. Wenn der veredelte Spinat an einen Händler weiterverkauft wird, werden wiederum beim Transport Informationen an die Blockchain übermittelt. Smart Contracts helfen dem Händler dabei sein Inventar immer auf dem optimalen Stand zu halten und eine Just-in-time-Planung durchzuführen. Wenn der Spinat sich nun bei einem Händler befindet, können Konsumenten vor Ort das Produkt einscannen und so alle vorher eingetragenen Informationen über das Produkt erfahren.

Wie hätte dieser aufwendige Prozess bei dem E. Coli Ausbruch helfen können?

Nachdem am 20. September 2006 das Produkt, welches den E.coli Ausbruch verursacht hat, identifiziert wurde, hätte es nur wenige Minuten gebraucht, um festzustellen woher der Spinat des beanstandeten Produktes stammt. Ein Blick in die Blockchain hätte genügt, um das Produkt bis zum Bauernhof genau zurück zu verfolgen. Dieser Unterschied von wenigen Minuten zu neun Tagen brachte für die Spinat-Bauern erhebliche wirtschaftliche Folgen mit sich. Sie konnten weiterhin ihre Produkte nicht verkaufen, obwohl sich im Nachhinein herausgestellt hat, dass ihr Spinat nicht befallen war. So hätten viele Bauern ihre Existenz erhalten können und das Risiko für die Menschen wäre schneller minimiert worden.
Auch das Risiko für die Länder, in die das infizierte Produkt exportiert wurde, hätte verringert werden können. In diesem Fall war das Produkt außerhalb der amerikanischen Grenzen nicht weiter verfolgbar. Wäre das Produkt auf einer Blockchain, hätte es noch genau verfolgt werden können und sofort aus dem Umlauf gebracht werden können.
Das betroffene Produkt hatte in diesem Fall nur einen Bestandteil, den Spinat. Viele Produkte setzen sich aus verschiedenen Inhaltsstoffen zusammen. Jeden dieser

Inhaltsstoffe auf traditionelle Weise zurück zu verfolgen würde weitaus länger als neun Tage dauern. Durch die Blockchain-Technologie wäre auch dies in wenigen Minuten machbar.

5.4 Kritik

Wenn neue Techniken vorgestellt werden, wird oftmals nur auf die positiven Aspekte geschaut. Jedoch sind sie nicht immer so weltbewegend und nützlich wie vermutet.

Die Implementierung neuer Techniken in ein Unternehmen bringt meistens hohe Umstellkosten mit sich. Um die Blockchain-Technologie in das SCM zu implementieren, muss nicht nur ein Unternehmen die neue Technik einführen und das Personal schulen, sondern jedes Unternehmen entlang der Wertschöpfungskette. Dies ist gerade für kleinere Unternehmen eine große Herausforderung, da denen oft Ressourcen wie Zeit, Geld und Personal fehlen.

Eine weitere Frage ist auch, ob alle Stellen entlang der Wertschöpfungskette gleich viel von der Einführung der Blockchain-Technologie profitieren. So profitiert der Lebensmittelhändler von sämtlichen Aspekten der Blockchain-Technologie, der Produzent an früher Stelle der Wertschöpfungskette jedoch nur von wenigen. Die Implementierung muss daher so leicht wie möglich gemacht werden. Kleinere Unternehmen und Unternehmen an früher Stelle der Wertschöpfungskette könnten Unterstützung in Form von Schulungen oder finanziellen Mitteln von Unternehmen, welche mehr von der Einführung profitieren, erhalten.

Wenn mehrere Unternehmen miteinander arbeiten und Informationen transparent austauschen, ist Datenschutz immer ein wichtiges Thema. Unternehmen sind vorsichtig mit wem sie ihre Informationen teilen. Konkurrenten können diese geteilten Daten nutzen, um dem Unternehmen zu schaden oder sich einen Vorteil zu verschaffen. Es ist daher wichtig, zu kontrollieren, welche Informationen für welche Gruppen sichtbar sind.

Unternehmen werden sich auch fragen, ob eine normale Datenbank mit bisheriger Sendeverfolgung nicht auch ausreichend ist. Bei kleineren Wertschöpfungsketten ist diese Frage durchaus begründet, da diese das Potential der Blockchain-Technologie

nicht vollständig ausschöpfen würden. Für komplexere und globale Wertschöpfungsketten sind die Vorteile jedoch signifikant.

In der folgenden Tabelle ist eine Gegenüberstellung einiger Faktoren von traditionellen Datenbanken mit bisheriger Sendeverfolgung und der Blockchain dargestellt.

Tabelle 2: Vergleich traditionelles Track&Trace mit der Blockchain

Traditionelles Track&Trace	**Blockchain**
Zentrale Datenbank, die von einem Spieler verwaltet wird – Abhängigkeit	Verteilte Datenbank/Ledger, auf die jeder Spieler unabhängig zugreifen kann
Nicht revisionssicher	Revisionssicher durch Design
Keine vollständige Validierung der Aktivitäten möglich	Vollständige Validierung aller Aktivitäten in der Supply Chain
Anfälligkeit gegenüber Cyberattacken, je nach Schutz der zentralen Datenbank	Hoher Schutz vor Cyberattacken aufgrund dezentraler Speicherung
Beschränkung auf T&T relevante Daten (Ort und Zeit)	Anreicherung der einzelnen Datensätze mit beliebigen Informationen
Begrenztes Automatisierungspotenzial, da Daten nicht revisionssicher sind und Abhängigkeit von Verwalter der Datenbank besteht	Hohes Automatisierungspotenzial durch Revisionssicherheit der Daten und Schnittstellenmöglichkeiten, z.B. für Apps

Quelle: In Anlehnung an: Online im Internet: Herzog, Cornelius; Oest, Philipp (2017): Blockchains in der Supply Chain. URL: https://www.oliverwyman.de/our-expertise/insights/2017/nov/blockchains-in-der-supply-chain.html (Abruf: 25.10.2018).

6. Blockchain im Gesundheitswesen

Die Blockchain-Technologie ist nicht nur im SCM verwendbar. Um die Breite der Möglichkeiten der Blockchain-Technologie darzustellen, wird in diesem Kapitel die mögliche Anwendung im Gesundheitswesen kurz dargestellt. Genauer gesagt geht es um die Dokumentation von Gesundheitsinformationen und die Verwaltung von Patientenakten.

Status quo werden Patientenakten von dem behandelnden Arzt geführt und aufbewahrt. Oftmals werden diese nicht elektronisch abgespeichert, sondern lokal in Kreditakten geführt. Wenn der Patient von anderen Ärzten oder im Ausland behandelt wird, haben diese oftmals keinen Zugriff auf die Patientenakte.[57]

Ein weiteres Problem ist der Zugriff auf die eigene Patientenakte. Patienten haben nur in Ansätzen Zugriff auf ihre Patientenakte und Kontrolle über ihre Daten. So ist es für einen Patienten nicht ohne Umstände möglich, seine Patientenakte einzusehen oder zu bestimmen, wem er für welche Zwecke seine Daten bereitstellt.

Die Blockchain-Technologie bietet eine Lösung zu diesen Problemen. Zur heutigen Zeit wird die Blockchain-Technologie noch nicht im Gesundheitswesen angewandt. Viele Unternehmen beschäftigen sich jedoch mit einer möglichen Implementierung. [58]

Eine Herangehensweise wäre, dass jeder Patient eine eigene öffentliche Patienten-ID auf der Blockchain erhält, welche nicht identifizierbar ist. Zu jeder Patienten-ID geht ein Patientenschlüssel einher, welcher benötigt wird, um Zugriff auf die Patientenakte zu gewähren. Wenn ein Patient bei einem Arzt untersucht wird, trägt dieser die Informationen nicht mehr in eine lokale Patientenakte ein, sondern in die Blockchain, auf welcher sich die Patienten-ID befindet. Die weitergeleiteten Informationen werden kryptographisch verschlüsselt, wodurch ein zweiter die Patientenakte nicht einsehen kann. Diese Informationen können nur mit dem

---

[57] Vgl. Krawiec, Rj u.a. (2017): Deloitte: Blockchain Einsatz im deutschen Gesundheitswesen S. 3. [online]. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/life-sciences-health-care/Blockchain_LSHC_komplett_Version_neu_safe.pdf (Abruf: 24.10.2018).

[58] Vgl. Winkler, Julia u.a. (2017): Blockchain: Die Demokratisierung des Gesundheitswesens? S. 14 f. [online]. URL: https://www.wig2.de/fileadmin/content_uploads/PDF_Dateien/White_Paper_Blockchain_-_Demokratisierung_des_Gesundheitswesens.pdf (Abruf: 24.10.2018).

passenden Patientenschlüssel gelesen werden. Da nur der Patient seinen Patientenschlüssel besitzt, hat er jederzeit Zugriff auf seine Patientenakte. Dadurch besteht die Möglichkeit selbst zu entscheiden, für wen er seine Daten bereitstellt. Die Daten können nach Belieben Gesundheitsorganisationen oder Institutionen zur Verfügung gestellt werden. Wenn der Patient seinen Arzt wechselt oder im Ausland bei einem Arzt ist, muss nicht erst über umständliche Verfahren die Patientenakte übermittelt werden. Der Patient gewährt vor Ort durch seinen Patientenschlüssel Einsicht in seine Daten.

Durch dieses Verfahren ist es auch möglich gegen gefälschte Rezepte vorzugehen. Der behandelnde Arzt trägt bei der Behandlung das ausgestellte Rezept in die Blockchain ein. Wenn der Patient dieses Rezept bei einer Apotheke einfordern will, muss er zunächst Einsicht auf die Eintragung des Rezeptes ermöglichen. Dadurch ist die Apotheke sicher, dass das Rezept nicht gefälscht ist und kann dem Patienten das verschriebene Produkt ausstellen. Der Apotheker würde einen Eintrag in die Blockchain vornehmen, welcher besagt, dass das Rezept eingelöst wurde. Dadurch kann ein Rezept nicht mehrmals verwendet werden.

Im Gesundheitswesen ist Datenschutz von sehr großer Bedeutung. Die Verlagerung aller Patientenakten auf eine öffentliche Blockchain ist daher kein leichter Schritt. Kryptographie hilft dabei Sicherheit in ein öffentliches Konstrukt zu bringen. Es gibt jedoch einige Risiken. Zum einen besteht keine weitere Möglichkeit die Patientenakte einzusehen, außer durch den Patientenschlüssel. Wenn der Patient verunglückt und nicht in der Lage ist Zugriff auf seine Patientenakte zu gewähren, ist es nicht möglich, für Ärzte diese einzusehen. Dadurch besteht die Gefahr, dass lebensrettende Informationen nicht zugänglich sind. Zum anderen besteht die Gefahr, dass der Patient seinen Patientenschlüssel verliert. Dadurch wäre er nicht mehr in der Lage seine Daten einzusehen und sie wären verloren.

7. Fazit

Unter Betrachtung der vier Kriterien für ein erfolgreiches SCM, wie in Kapitel 5 aufgeführt, ist deutlich zu erkennen, dass die Blockchain-Technologie das SCM positiv verändern kann.

Drei dieser Erfolgskriterien sind Flexibilität, Transparenz und Aktualität der Informationen. Durch die komplette Transparenz entlang der Wertschöpfungskette, sind eingetragenen Informationen direkt für jeden Teilnehmer der Blockchain sichtbar. Alle beteiligten Unternehmen sind daher in der Lage flexibler und effizienter zu arbeiten. Veränderungen oder unplanmäßige Ereignisse werden sofort identifiziert, wodurch Unternehmen Gegenmaßnahmen einleiten können. Bekannte Probleme wie das Auftreten des Ripple- oder Bullwhip-Effekts können dadurch verhindert werden. Smart-Contracts unterstützen Unternehmen dabei, indem sie aus den Daten der Blockchain Prognosen und Produktionsvorschläge erstellen. Aufgaben wie die Bezahlung von Lieferungen und das Management des Inventares können durch Smart-Contracts automatisiert werden.

Auch der Endkonsument profitiert von der Transparenz der Wertschöpfungskette. So wird er vor Fälschungen geschützt und ist in der Lage den Ursprung von Produkten zurückzuverfolgen. Unsicherheiten über Bio- und Fair-Trade-Produkte werden dadurch beseitigt.

Das vierte Erfolgskriterium ist die Kooperation der Unternehmen entlang einer Wertschöpfungskette. Damit die Blockchain-Technologie erfolgreich in ein SCM integriert werden kann, müssen alle Teilnehmer entlang der Wertschöpfungskette die neue Technik implementieren und miteinander kooperieren. Dies führt zu zusätzlichen Kosten für jedes beteiligte Unternehmen, allerdings profitiert nicht jeder Teilnehmer gleich viel von der Einführung. Dadurch können Konflikte zwischen den verschiedenen Teilnehmern entstehen. Wenn jedoch eine erfolgreiche Implementierung stattfindet wird das Vertrauen unter den Teilnehmern durch die kryptographische Grundlage der Blockchain und ihrer dezentralen und nicht manipulierbaren Funktionsweise verstärkt.

Die Blockchain-Technologie hat nicht nur das Potential ausschließlich im SCM implementiert zu werden. Im Gesundheitswesen gibt es erste Pioniere, welche an

einer möglichen Implementierung arbeiten. So kann ein weltweit einheitliches System für die Führung von Patientenakten erstellt werden, welches den Patienten volle Kontrolle über ihre Akten gewährt.

Wie bei jeder neuen Technologie gibt es auch bei der Blockchain-Technologie noch viele Probleme und stets neue Herausforderungen. Unternehmen wie Walmart machen durch ihre Implementierung den ersten Schritt und erkennen das Potential dieser neuen Technologie. In der nahen Zukunft besteht die Möglichkeit auch in deutschen Supermärkten oder in anderen Anwendungsfeldern die Blockchain-Technologie vorzufinden.

Literatur- und Quellenverzeichnis

Bücher

-Berentsen, Aleksander; Schäfer, Fabian (2017): Bitcoin, Blockchain und Kryptoassets Eine umfassende Einführung, 1. Auflage, (BoD), Norderstedt

-Buchmann, Johannes (2001): Einführung in die Kryptographie, 2. Auflage, (Springer), Berlin Heidelberg

-Gupta, Manav (2017): Blockchain For Dummies, IBM Limited Edition, (John Wiley & Sons, Inc.), Hoboken

-Hoffmann, Erik; Strewe, Urs Magnus; Bosioa, Nicola (2018): Supply Chain Finance and Blockchain Technology, (Springer), Cham

-Ivanov, Dmitry (2018): Structural Dynamics and Resilence in Supply Chain Risk Management, (Springer), Cham

-Karpfinger, Christian; Kiechle, Hubert (2010): Kryptologie Algebraische Methoden und Algorithmen, 1. Auflage, (Vieweg + Teubner), Wiesbaden

-Laurence, Tiana (2018): Blockchain für Dummies, (WILEY), Weinheim

-Morabito, Vincenzo (2017): Business Innovation Through Blockchain, (Springer), Cham

-Narayanan, Arvind u.a. (2016): Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, (Princeton University Press), Princeton

-Paar, Christof; Pelzl, Jan (2016): Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender, (Springer), Berlin Heidelberg

-Schelthoff, Christof (2010): Diskrete Mathematik Diskrete Strukturen & Zahlentheorie, (FH Aachen – Campus Jülich), Aachen

-St Denis, Tom; Johnson, Simon (2017): Kryptografie für Entwickler Das erste umfassende Kryptografie-Handbuch für Software-Entwickler, (Franzis), Haar bei München

-Werner, Hartmut (2017): Supply Chain Management Grundlagen, Strategien, Instrumente und Controlling, 6. Auflage, (Springer), Wiesbaden

Internetquellen

-Cant, Bart u.a. (2017): Smart Contracts in Financial Services: Getting from Hype to Realtiy, Online im Internet: URL: <https://www.capgemini.com/wp-content/uploads/2017/07/smart_contracts_in_fs.pdf> (Abruf: 09.10.2018)

-Chen, Si u.a. (2017): A Blockchain-Based Supply Chain Quality Management Framework, Online im Internet: URL: <https://www.researchgate.net/publication/321027278_A_Blockchain-Based_Supply_Chain_Quality_Management_Framework> (Abruf:10.10.2018)

-DBS Asian Insights (2016): Understanding Blockchain Technology And What It Means For Your Business, Online im Internet: URL: <http://www.dbs.com.sg/treasures/aics/pdfController.page?pdfpath=/content/article/pdf/AIO/AIO_2016/SECTOR-19-001-blockchain-lowres.pdf> (Abruf: 18.10.2018).

-G. Kwon, Ik-Whan; Suh, Taewon (2006): Facotrs Affecting the Level of Trust and Commitment in Supply Chain Realtionships, Online im Internet: URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745- 493X.2004.tb00165.x> (Abruf: 09.10.2018)

-Galvin, David (2017): IBM and Walmart: Blockchain for Food Safety, Online im Internet:
URL: <https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf> (Abruf: 09.10.2018)

-Herzog, Cornelius; Oest, Philipp (2017): Blockchains in der Supply Chain, Online im Internet: URL: https://www.oliverwyman.de/our-expertise/insights/2017/nov/blockchains-in-der-supply-chain.html (Abruf: 25.10.2018)

-IBM Institute for Business Value (2016): Trust in trade Toward stronger supply chains, Online im Internet: URL: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN> (Abruf: 09.10.2018)

-IHK-Wirtschaft in Mittelfranken (2005): Welche Folgen hat die Produktpiraterie?, Online im Internet: URL: <https://www.ihk-nuernberg.de/de/IHK-Magazin-WiM/WiM-Archiv/WIM-Daten/2005-12/Wirtschaftsfragen/Welche-Folgen-hat-die-Produktpiraterie-.jsp> (Abruf: 09.10.2018)

-Krawiec, Rj u.a. (2017): Deloitte: Blockchain Einsatz im deutschen Gesundheitswesen, Online im Internet: URL: <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/life-sciences-health-care/Blockchain_LSHC_komplett_Version_neu_safe.pdf> (Abruf: 24.10.2018)

-Kauffmann, Rémy; Zehnder, Patrick (2017): Geschichte der Kryptographie, Online im
Internet: URL: https://www.swisseduc.ch/geschichte/kryptographie/docs/script_kryptographie_swisseduc.pdf (Abruf: 18.10.2018)

-Kopecka, Jarmila; Penner, Guido; Santema, Sicco (2002): Flexibility in supply chain managment, Online im Internet: URL: https://www.impgroup.org/uploads/papers/7315.pdf (Abruf: 17.10.2018)

-Jayachandran, Praveen (31.05.2017): The difference between public and private blockchain, Online im Internet: URL: <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/> (Abruf: 09.07.2018)

-Lewis, Antony (29.10.2015): A Gentle Introduction To Blockchain Technology, Online im
Internet: URL: <https://assets.ctfassets.net/sdlntm3tthp6/1N6VBCrkp6oywIooC20omQ/9b93ac6ac921743a38f80aaeb823a102/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf> (Abruf: 09.10.2018)

-Metzger, Jochen (19.02.2018): Distributed Ledger Technologie (DLT), Online im Internet: URL: <https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444> (Abruf: 09.07.2018)

-Mitschele, Andreas (19.02.2018): Smart Contract, Online im Internet: URL: <https://wirtschaftslexikon.gabler.de/definition/smart-contract-54213/version-277263> (Abruf: 09.07.2018)

-Mitschele, Andreas (28.10.2016): Blockchain, Online im Internet: URL: <https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-188335> (Abruf: 09.07.2018)

-Mullaney, Ryan (2018): Blockchain becomes a crucial link in the supply chain, Online im Internet: URL: <https://aqurus.ca/blockchain-crucial-link-supply-chain> (Abruf: 25.10.2018)

-Mücke, Thomas (16.04.2018): Genesis Block, Online im Internet: URL: <https://www.coin-report.net/de/genesis-block/> (Abruf: 18.10.2018)

-Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, Online im Internet: URL: <https://bitcoin.org/bitcoin.pdf> (Abruf:22.10.2018)

-Primärquelle von de.statista.com (2016): Bevölkerung in Deutschland nach Einstellung zur Aussage „Ich bin auch bei Produkten des täglichen Lebens sehr anspruchsvoll“ von 2013 bis 2016 (in Millionen), Online im Internet: URL: <https://de.statista.com/statistik/daten/studie/172161/umfrage/einstellung-hoher-anspruch-auch-bei-alltaeglichen-produkten/> (Abruf: 09.10.2018)

-Primärquelle von de.statista.com (2018): Umsatz mit Bio-Lebensmitteln weltweit in den Jahren 1999 bis 2016 (in Milliarden US-Dollar), Online im Internet: URL: <https://de.statista.com/statistik/daten/studie/187590/umfrage/weltweiter-umsatz-mit-bio-lebensmitteln-seit- 1999/> (Abruf: 09.10.2018)

-Primärquelle von de.statista.com (2017): Umsatz mit Fairtrade-Produkten weltweit in den Jahren 2004 bis 2016 (in Millionen Euro), Online im Internet: URL: <https://de.statista.com/statistik/daten/studie/171401/umfrage/umsatz-mit-fairtrade-produkten-weltweit-seit- 2004/> (Abruf: 09.10.2018)

-The Food Industry Center, University of Minnesota; National Center for Food Protection and Defense (2009): Natural Selection: 2006 E. coli Recall of Fresh Spinach A Case Study by The Food Industry Center, Online im Internet: URL: <http://ageconsearch.umn.edu/bitstream/54784/2/Natural%20Selection.pdf> (Abruf: 09.10.2018)

-Voigt, Kai-Ingo u.a. (19.02.2018): Supply Chain Management (SCM), Online im Internet: URL: <https://wirtschaftslexikon.gabler.de/definition/supply-chain-management-scm-49361/version-272597> (Abruf: 09.10.2018)

-Winkler, Julia u.a. (2017): Blockchain: Die Demokratisierung des Gesundheitswesens?, Online im Internet: URL: <https://www.wig2.de/fileadmin/content_uploads/PDF_Dateien/White_Paper_Blockchain_-_Demokratisierung_des_Gesundheitswesens.pdf> (Abruf: 24.10.2018)

-World Health Organization (2017): 1 in 10 medical products in developing countries is substandard or falsified, Online im Internet: URL: <http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified> (Abruf: 09.10.2018)

Eidesstattliche Versicherung

van Unen, Simon

Name, Vorname

Ich versichere hiermit an Eides statt, dass ich die vorliegende Abschlussarbeit mit dem Titel:

„Kritische Betrachtung ausgewählter Einsatzgebiete der Blockchain-Technologie unter besonderer Berücksichtigung des Supply-Chain-Managements“

selbstständig und ohne unzulässige fremde Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Ort, Datum, Unterschrift