Hausarbeit

Bedingheiten und Möglichkeiten von Blockchain-Technologien im betriebswirtschaftlichen Einsatz

Christian Eberling

Matrikelnummer: 3718725
Betreuer: Prof. Dr. Gräbe
Abgabedatum: 15.05.2019

Inhaltsverzeichnis

1 Einleitung **2**

2 Verteilte Systeme **3**

3 Distributed Ledger Technology und Blockchain **4**

3.1 „Open-Public“ Ledger Systeme 5

3.1.1 Blockchain 7

3.1.2 Konsensmechanismus 8

3.1.3 Entlohnung 11

3.2 Eingeschränkte Blockchain Systeme 11

4 Anwendungsbeispiel: Supply-Chain Management **12**

5 Zusammenfassung **17**

1 Einleitung

Innovation und stetige Weiterentwicklung sind Teil des wirtschaftlichen Wachstums. Technologien zur Verbesserung von betriebsinternen Strukturen sowie den interstrukturellen Mechanismen auf dem globalen Markt sind Teil der heutigen Weltwirtschaft. Das Streben nach stetiger Verbesserung treibt die globale Unternehmenslandschaft an, neue Technologien sollen Kosten einsparen, Prozesse beschleunigen und sicherer machen. So erscheint es, als würde jede neue Idee das Potenzial für eine bessere Welt mit sich bringen. So auch die „Blockchain“: sie beinhalte ein neues Innovationspotenzial, ähnlich wie das des Internets in den 90er Jahren.[1] So entstehen Start-Ups mit neuen Anwendungsideen auf der Suche nach Investoren, um altbackene Infrastrukturen zu revolutionieren: dank neuer Blockchain Technologien sollen gesamte Industriezweige umstrukturiert werden können. Die Blockchain sei ein Versprechen an Sicherheit, Transparenz und Integrität von jeglichen Daten. Durch die Dezentralisierung werden Intermediäre redundant und abgelöst mathematischer Berechenbarkeit, „Hauptsache Blockchain“ ist die Devise. Eine Vielzahl von technischen Innovationen entstehen währenddessen in der Blockchainsphäre. „Atomic Swaps“, „Zero-Knowledge-Beweise“ und „Lightning-basierte Smart Contracts“ sollen Software Entwicklern bei der Realisierung von sicheren und privaten Werttransaktionen verhelfen. Versucht man sich erst einmal einen groben Überblick über die Kryptosphäre zu verschaffen, so kann das Mithalten mit Neuerungen schier unmöglich erscheinen. In dieser Arbeit wird zuerst eine allgemeine Definition von verteilten Systemen aufgestellt, die als Basis für Distributed Ledger Technologien und letztlich Blockchain Systemen dient. Für jene wird ein grundlegender Überblick über essentielle Mechanismen und Strukturen gegeben, wie sie in Ihrer ursprünglichen Idee entwickelt wurden. Letztlich wird eine potenzielle Anwendung von Blockchain im Unter-

[1] Vgl. Swan M. (2015): Blockchain - Blueprint for a New Economy S.7

nehmensbereich angeführt und Herausforderungen sowie Möglichkeiten der Idee diskutiert.

2 Verteilte Systeme

Im Forschungsfeld der Informatik bestehen verteilte Systeme aus einzelnen unabhängigen autonomen Einheiten, die dem Nutzer wie ein kohärentes Ganzes erscheinen. Nach Tanenbaum und Van Steen sollten diese Systeme grundsätzlich offen, kollaborativ und skalierbar sein.[2] Typischerweise werden verteilte Systeme für die effiziente Verfügbarkeitmachung von Rechenleistung und Speicherkapizität verwendet. Charakteristisch für verteilte Systeme, die zur Bereitstellung von Daten verwendet werden, ist die Anwesenheit mehrerer Computer, die innerhalb eines Netzwerkes über ein Kommunikationsprotokoll einen einheitlichen Zustand von Daten erhalten. Verteilte Systeme sind aufgrund der nötigen Synchronisation der einzelner Einheiten, der Erhaltung der Konsistenz, der Replikation der Zustände und dem Fehlertoleranzmanagement gegenüber nicht verteilten Systemen grundsätzlich komplexer. Verteilte Systeme haben typischerweise eine kleinere Kommunikationsbandbreite, unabhängige Fehlerwahrscheinlichkeiten für jedes Teilsystem und potenzielle Kommunikationsverzögerungen. Die Erwägung einer solchen Architektur muss daher begründet sein und zieht kritische technische Entscheidungen und Kompromisse mit sich.[3] Nach dem CAP-Theorem von Brewer ist es innerhalb eines verteilten Systems beispielsweise nicht möglich, vollkommene Konsistenz, Verfügbarkeit und Ausfalltoleranz gleichzeitig zu garantieren.[4] Für die Rechtfertigung eines solchen technischen Aufwands werden einfachere Skalierbarkeit, höhere Modularität und verbesserte Kostenfaktoren als

[2] Vgl. Tanenbaum et al. (2006): Distributed Systems: Principles and Paradigms S.3
[3] Vgl. Tanenbaum et al. (2006): Distributed Systems: Principles and Paradigms S.5
[4] Vgl. https://de.wikipedia.org/wiki/CAP-Theorem [08.08.2019]

Argumente genannt.[5]

3 Distributed Ledger Technology und Blockchain

Allgemein betrachtet sind Distributed Ledger Systeme Datenbanken, die in Ihrer Architektur auf verteilten Systemen aufbauen. „Distributed“ bezieht sich hierbei zunächst auf die geographische und architektonische Verteilung zusammengeschlossener Computer: mehrere unabhängige Geräte oder „nodes“ werden innerhalb eines Netzwerkes verbunden und können durch das Empfangen und Senden von Nachrichten direkt miteinander kommunizieren.[6] Jede Node verhält sich generell gleich: sie speichert eine gesamte Kopie des Datenbankzustands (Ledgers) und synchronisiert Aktualisierungen autonom, indem der Kommunikationskanal im Netzwerk auf Datenbankveränderungen abgehört wird und an alle benachbarten Nodes weiterkommuniziert wird, sodass im Idealfall ein allgemeingültiger Zustand innerhalb des Netzwerks erreicht wird und alle Nodes dieselbe, gesamte Kopie der Datenbank gespeichert haben. DLT Systeme sind keine neue Technologie an sich, sondern eine Kombination aus unterschiedlichen Technologien und können je nach Anspruch an Dezentralität und Performanz fundamental unterschiedliche Strukturen aufweisen. Hierbei geht es nicht nur wie eben um Dezentralität im Sinne geographischer oder physischer Gegebenheiten der Geräte, sondern auch um die Frage nach Kontrolle darüber, wer Zugangs- und Teilnahmeberechtigung am Netzwerk hat und Entscheidungen über das Systemproto-

[5] Vgl. Tanenbaum et al. (2006): Distributed Systems: Principles and Paradigms S.5

[6] Vgl. https://medium.com/@shyamshankar/ centralized-ledgers-vs-distributed-ledgers-layman-understanding-52449264ae23 [08.08.19]

koll und den Datenzustand treffen kann.[7] Einmal wird zwischen „permissionless“ oder „permissioned“ Distributed Ledgern unterschieden. Hierbei geht es um Schreibberechtigungen und somit implizit um das Mitbestimmungsrecht über die allgemeingültige Richtigkeit der Daten. In permissionless Distributed Ledger Netzwerken gibt es keine einzelne Instanz, die die Teilnahme am Netzwerk einschränken kann - jeder kann sich mit dem Netzwerk verbinden oder trennen, eine Kopie der Datenbank speichern und gemäß des Netzwerkprotokolls Veränderungen in den Ledger eintragen und über die Legitimität der Veränderungen anderer Teilnehmer mitbestimmen.[8] Wird zwischen „public“ oder „private“ Distributed Ledgern unterschieden, so betrachtet man hingegen die Leseberechtigung und die transparente Einsicht in die Daten. In öffentlichen (public) verteilten Distributed Ledgern sind die Daten uneingeschränkt einsehbar. Eine Identität zur Authentifizierung wird hierbei obsolet. In privaten Distributed Ledgern wird die Einsicht und Transparenz in die Daten grundsätzlich über eine entscheidende Partei eingeschränkt und erfordert eine Authentifizierung, um den Zugang auf verifizierte Teilnehmer einzugrenzen. Je nach Anspruch an das System prägen die Kombinationen unterschiedlicher Technologien daher zu fundamental verschiedenen Charakteristika des DLT Systems und implizieren oft große Unterschiede in ihrer Stabilität, Sicherheit und Performanz, vorallem aber in Ihrer Nützlichkeit in unterschiedlichen Anwendungsfällen.

3.1 „Open-Public“ Ledger Systeme

Herausforderungen eines uneingeschränkt mitbestimmbaren und öffentlich einsehbahren Ledger Systems entstehen vorallem in der Koordinierung des

[7] Vgl. https://consensys.net/academy/blockchain-basics-book/principles-of-decentralization [08.08.19]

[8] Vgl. https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains [08.08.19]

Netzwerks. Gerade weil keine zentrale Kontrollinstanz oder dritte Partei im gleichberechtigten „peer-to-peer“ Netzwerk existiert, müssen Regeln definiert werden, die zur Erhaltung eines allgemeingültigen Zustand der Datenbank führen. Open-Public Ledgersysteme fallen daher in Ihrer Umsetzung tendenziell komplexer aus - nicht zuletzt weil man bei Systemen öffentlich zugänglicher Art von „malicious nodes“ im Sinne von Akteuren ausgehen muss, deren Interessen nicht mit der Mehrheit des Netzwerks konvergieren. Durch die Kombination von spieltheoretischer Anreizstukturen im Sinne der Mechanismus-Design-Theorie und kryptographischen Verfahren wie dem Hash-Algorithmus (SHA) und der Public-key Verschlüsselung wird daher in der Forschung versucht, das fundamentale Probleme in offenen dezentralisierten verteilten Systemen zu lösen: die Verifizierbarkeit und Manipulationssicherheit von Datenzuständen sowie die Erhaltung von Kooperation und Vertrauen innerhalb des Netzwerks ohne zentraler Kontrollinstanz zwischen einander unbekannten Parteien.[9] [10] [11] Dadurch werden nicht nur geographisch „dezentrale“ Systeme, also im Sinne physischer Gegebenheiten des Netzwerkes möglich, sondern auch eine „politische“ Dezentralisierung hinsichtlich der Kontrolle über den allgemeingültigen Zustand der Daten von Distributed Ledgern möglich. [12] [13] Im Falle von Blockchain Systemen, die in Ihrer ursprünglichen Entwicklung als öffentliche und offene, politisch dezentralisierte Ledger Plattform verstanden wurden(Mastering Blockchain p12), seien somit

[9] Vgl. https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf [08.08.2019]

[10] Vgl. https://media.consensys.net/blockchain-vs-distributed-ledger-technologies-1e0289a87b16

[11] Vgl. Bonneau et al. (2016): Bitcoin Cryptocurrency Technologies: A Comprehensive Introduction S.73

[12] Vgl. Bonneau et al. (2016): Bitcoin Cryptocurrency Technologies: A Comprehensive Introduction S.95

[13] https://consensys.net/academy/blockchain-basics-book/principles-of-decentralization

Kooperation und Vertrauen innerhalb eines öffentlichen und offenen Systems möglich und enthalte somit das Potenzial zur neutralen, zensurresistenten und grenzüberschreitenden Austauschplattform von Informationen und Werten. [14]

3.1.1 Blockchain

Wird heutzutage der Begriff Blockchain mit DLT Systemen in Zusammenhang gebracht, so beschreibt der Begriff im ursprünglichen Sinne eigentlich zuerst einmal nur die zugrunde liegende Methodik von Datenspeicherung: eine append-only Datenstruktur zur Speicherung und Organisierung von Informationen. Diese Datenstruktur kann allerdings in DLT Systemen sinnvolle Vorteile bringen, die später erläutert werden. Technisch betrachtet besteht die Blockchain Datenstruktur aus einer linear geordneten, rückwärts verketteten Liste von konstant großen Datensätzen oder „Blöcken“. Jeder Block besitzt dabei eine einzigartig identifizierende Prüfsumme oder „Hash“. Hier kommt bereits das erste kryptographische Verfahren der Blockchain zu tragen, denn mithilfe eines Hashbaumes wird die Prüfsumme von den blockeigenen Daten abhängig gemacht. Bedeutend hierbei ist, dass das Verändern der Daten innerhalb des Blockes immer zu einer Veränderung der ursprünglichen Prüfsumme oder Hash des Blockes führt und somit durch Erkennbarmachung einer Inkongruenz eine unbemerkte, nachträgliche Manipulation der Daten verhindert. Im selben Sinne verwendet man den Hash auch als Hashzeiger für die Verkettung der Datenblöcke: dabei wird der Hash des aktuellen Blockes in die Kopfzeile des jeweils nächsten Blockes gespeichert. Es entsteht somit eine integritätserhaltende, chronologisches Reihenfolge der Blöcke, da wie auch beim Hashbaum innerhalb eines Blockes, eine nachträgliche Änderung eines vorhergenden Blockes aufgrund der Verkettung alle Prüfsummen

[14] Vgl. https://markshirecrypto.com/cryptocurrency/the-five-pillars-of-cryptocurrency/ [12.09.2019]

der nachfolgenden Blöcke verändern würde. Der fundamentale Vorteil dieses Datenspeicherformats liegt in der Integritätsprüfung: das Vergleichen des Hashes im aktuellsten Block reicht, um die gesamte Vergangenheit der Datenzustände zweier Ledgerkopien, beispielsweise in einem Netzwerk, auf Gleichheit zu überprüfen und erspart das zeitaufwendige Vergleichen jedes Bytes zwischen zwei Datensätzen. Werden Blockchains oftmals mit Transparenz, Sicherheit und Unveränderbarkeit assoziert, so muss zuerst einmal genauer definiert werden, in welchem Kontext dieser Begriff verwendet wird - handelt es sich um ein verteiltes Ledger System mit Blockchain Datenstruktur, so sind unter anderem die zugrundeliegende Architektur und Regeln des Systems, aber auch Teilnehmergröße und Dezentralisierungsmechanismen unvernachlässigbar für die Bewertung der Transparenz, Sicherheit und Integrität der gespeicherten Daten - mehr dazu später.[15][16]

3.1.2 Konsensmechanismus

Die Erhaltung eines allgemeingültigen Zustands der Daten oder eines „Konsens“ in DLT Systemen, welcher durch kooperatives Verhalten zwischen allen „honest“ Nodes (also Nodes, die zur Mehrheit des Netzwerkes gehören und im Sinne des Protokolls handeln) bedingt ist, wird in dezentralisierten peer-to-peer Ledger Systemen anders als in zentralisierten Systemen gelöst. Netzwerkstörungen und hohe Latenzen, Geräteausfälle und absichtliche Untergrabungen durch „malicious“ nodes können zu Unstimmigkeiten in Teilen des Netzwerks führen. Ohne zentraler Entscheidungsinstanz müssen hierbei Synchronisationsregeln definiert werden werden, um einen einheitlichen und legitimen Datenzustand zu erreichen. Eine typische Schwachstelle in peer-to-peer

[15] Vgl. https://www.coindesk.com/bitcoin-and-blockchain-the-tangled-history-of-two-tech-buzzwords [09.08.2019]

[16] Vgl. https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains [09.08.2019]

Systemen mehrheitsbestimmter Art wie es in dezentralisierten peer-to-peer Ledgersystemen der Fall ist, ist die Resistenz gegen Sybil Attacken, bei denen einzelne Individuen beispielsweise durch das Erstellen mehrerer falscher Identitäten versuchen, einen mehrheitlichen Kontrolleinfluss über die Systemorganisation zu erhalten.[17] Während dies in zentralisierten Systemen durch Authentifizierungssysteme und Zugangseinschränkungen gelöst werden kann, erweist sich dies in zugangunbeschränkten, offenen Systemen als komplexer. Eine Lösung für dieses Problems findet sich im Proof-of-Work Verfahren, ein dynamisch angepasster, spieltheoretischer Konsensalgorithmus, bei dem die Sicherheit und Stabilität des dezentralisierten Systems mit zumender Anzahl an Teilnehmern wächst.

Hierzu wird eine Anreizstruktur spieltheoretischer Art technisch umgesetzt, die eine organisationserhaltende Kooperation dadurch gewährleistet, dass einerseits die Teilnahme am DLT mit einem Kostenaufwand verbunden ist und das kooperative Verhalten für das selbstinteressierte Individuum immer mehr lohnt als das unkooperative Verhalten.

Auf technischer Ebene passiert folgendes: Jede Node schreibt neue Daten aus einem Pool noch nicht verifizierter Daten zunächst in einen Datensatz (Block) und versucht für diesen Block so schnell wie möglich eine neue Prüfsumme zu generieren. Dabei wird entsprechend des Konsensprotokolls die Berechnung der Prüfsumme durch mathematische Anforderungen so erschwert, dass mit einer hohen Wahrscheinlichkeit erst nach einem bestimmten Zeit- und Rechenaufwand eine Prüfsumme gefunden werden kann, die den Anforderungen entspricht. Dadurch garantiert das System, dass die Teilnehmer einen Kostenaufwand in Form von Rechenleistung und implizit Energie aufgewendet haben müssen, um die Prüfsumme generiert zu haben. Schafft es ein Teilnehmer, eine Prüfsumme zu generieren, die den Anforderungen ent-

[17] Vgl. Vukolic (2015): The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication

spricht, propagiert dieser den Datenblock samt Prüfsumme über das Netzwerkprotokoll und die restlichen Teilnehmer im Netzwerk überprüfen die Daten auf Gültigkeit. Die geringen Kosten zur Überprüfung der Gültigkeit sind dabei asymmetrisch zu den Generierungskosten einer Prüfsumme und können vom gesamten Netzwerk schnell durchgeführt werden. Erfüllt der Block und die enthaltenen Daten alle vom Konsensprotokoll bedingten Regeln, übernehmen alle Nodes den neuen Block in die eigene Kopie der Blockchain. Die Node, die die Prüfsume zuerst gefunden und propagiert hat, wird daraufhin gemäß einer Anreizstruktur entlohnt und der Prozess beginnt von vorne. Aus dem Eigeninteresse der Teilnehmer, für aufgewendete Ressource entlohnt zu werden, den Regeln konform zu handeln und Daten in die Blockchain entsprechend des Protokolls zu speichern, gehen die Datenspeicherung, die Sicherheit sowie die Integrität des Systems indirekt hervor. Wichtig ist, dass die Schwierigkeit der Anforderungen an die Prüfsumme proportional zur Rechenleistung des Gesamtsystems angepasst wird, um einen möglichst konstanten Zeitabstand zwischen Blockgenerierungen zu erzielen. Je größer das Netzwerk und je mehr Rechenleistung im Gesamtnetzwerk durch einzelne Teilnehmer zu Verfügung stehen, desto schwieriger werden die Anforderungen an die zu generierende Prüfsumme, um die Blockgenerierungszeit konstant zu halten. Dies verbessert einerseits den Schutz gegen Sybil Attacken, da der Angreifer eine immer höhere Rechenleistung aufwenden muss, um mehrheitliche Kontrolle über den Konsens zu erhalten, andererseits erlaubt gerade die zeitliche Verzögerung der Blockgenerierung das Auflösen von Diskrepanzen im Netzwerk und der Sicherstellung der Validität der Daten. Entstehen Diskrapenzen im Netzwerk, beispielsweise seien alle Nodes aufgrund von Latenzstörungen in zwei Gruppen mit jeweils einem für sie gültigen Zustand aufgeteilt, so wird grundsätzlich die Länge der Blockchain vom Zeitpunkt der Divergenz der Versionen entscheidend verwendet, um einen Konsens zu finden. Die Länge der Blockkette impliziert nämlich einerseits die Menge an aufgewendeter

Rechenleistung und somit implizit die proportionale Anzahl an Teilnahme des Gesamtnetzwerks. Eine mehrheitliche Partizipation der Teilnehmer an einem Zustand kann bei gleicher Prüfsummenanforderung eine längere Kette generieren und garantiert sich ihr Recht als legitime Blockkette. Je größer die Differenz zweier Blockketten, desto eindeutiger wird, welche Blockchain-Kette als legitime Kette gilt. Außerdem gehen verbrauchte Rechenleistung an der kürzeren und letztlich verworfenen Kette verloren, weswegen es einen Anreiz für Nodes gibt, stets zur mehrheitlichen Blockchain dazuzugehören. Ein Effekt, der den Zusammenhalt des dezentralisierten Systems mit sich bringt.

3.1.3 Entlohnung

Wird hier nicht weiter auf die Anreizstruktur im System eingegangen, so sei noch erwähnt, dass anhand des Beispiels von offenen dezentralisierten Kryptowährungen diese intrinsisch durch die Implementierung von nicht duplizierbarem, endlichen, nachverfolgbaren und tauschbaren Guthaben gelöst wird. Guthaben wird in kryptographisch gesicherten Addressen auf der Blockchain gespeichert. Zugangsberechtigung erhält man über eine geheimzuhaltende Prüfsumme, die beispielsweise zur Durchführung von Transaktionen benötigt wird. Entlohnt werden Nodes dann beispielsweise in Form von Transaktionsgebühren für das Aufnehmen und Validieren von Transaktionen in die Blockchain.

3.2 Eingeschränkte Blockchain Systeme

Halten wir also ein offenes dezentralisiertes Blockchain System fest: ein konsensbasiertes, teilnahmeuneingeschränktes Netzwerk aus Rechnern, dass durch das Zusammenspiel von kryptographischen Verfahren und spieltheoretischen Algorithmen eine Datenbank zur Verfügung stellt, dessen Integrität und Ver-

änderbarkeit durch festgelegte Protokolle gesichert sind.[18] Demgegenüber findet man entweder voll oder teilweise private und zugangseingeschränkte DLT Ansätze. Innerhalb des Netzwerks gibt es dabei grundsätzlich eine Kontrollinstanz, die über den Zugang entscheidet.[19] Beispielsweise sei der Zugang auf 15 Finanzinstitute eingeschränkt, von denen jede eine Node führt und von denen mindestens 10 einen Block validieren müssen bevor dieser gültig ist. Leseberechtigungen könnten dabei öffentlich sein oder ebenfalls eingeschränkt. sein.[20]

4 Anwendungsbeispiel: Supply-Chain Management

Keeping track of the material flow at each step, along with the corresponding paper flow, is a major undertaking that requires manual processes that are subject to human error, loss, damage or even theft and fraud (Harris 2016). For example, Provenance—a London-based startup—offers a Blockchain-based application that provides chain of custody along the supply chain for a given product or item. Information is open to end customers to prove the authenticity and provide assurance against counterfeits, and the product can be tracked along the supply chain. Another potential application is provided by smart contracts and crypto- graphic multi-signatures for all the various documentation and processing stages involved in a trade transaction (EBA 2015, p. 14). For example, a documentary trade could be ruled on a Blockchain, and execution of the payment to a vendor could be automated when

[18] Vgl. Bonneau et al. (2016): Bitcoin Cryptocurrency Technologies: A Comprehensive Introduction S.73

[19] Vgl. https://en.wikipedia.org/wiki/Blockchain [09.08.2019]

[20] Vgl. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [12.08.2019]

certain criteria is met [e.g. goods have been received or shipped or a particular date has been reached, (EBA 2015, p. 14)]. The transfer of title would be secure due to being triggered by a smart contract representing pre-set contractual agreements (Camerinelli 2016, p. 10). Furthermore, Wave Inc.—an Israeli-based startup—is creating a product that aims to take the place of traditional bills of lading using the Bitcoin Blockchain. It aims to replicate the industry standard workflows but replace printed documents with versions that are stored electronically in Blockchain transaction metadata, managing the ownership of each document or good in transport (Bauerle 2016, p. 13). Other solutions, such as the IBM's autonomous decentralized peer-to-peer telemetry (ADEPT), propose an even higher integration level by combining internet of things (IoT) with BCTs. Right from the time that a product completes final 5.2 Layers of Blockchain-Driven Supply Chains 65 assembly, it can be registered into a Blockchain representing its beginning of life so that the product remains a unique entity within that Blockchain throughout its life when it passes from owner to owner (IBM 2015, p. 6). In such a Blockchain-based IoT, there is the possibility of maintaining product information, its history, product revisions, warranty details and end of life, transforming the Blockchain into a trusted database. IBM (2015) also postulates the possibility of devices and products that engage in autonomous transactions and form records. The potential of having all the information written in a Blockchain allows the creation of an authoritative record that can be used to automatically establish smart contracts. Without such an authoritative record, smart contracts written on a Blockchain could hardly be executed, because parties need to agree on data and information that, like smart contracts themselves, are agreed to by a whole network through a consensus mechanism. The one-layer Blockchain solution sees as such a fully integrated and automated trade network where documents and goods are transparently identified and tracked along the supply chain. Because the information is registered on a

distributed database, it makes it tamper-resistant and fosters greater trust in the trade network.

Der Begriff „Supply Chain“, auf deutsch „Lieferkette“, beschreibt ein System aus Lieferanten, der Logistik, den Endkunden und dem Fluss von Rohstoffen und Waren zwischen involvierten Teilnehmern und bezieht zunehmend auch den Fluss von Informationen zwischen Akteuren in einem logistischen System mit ein.[21] Supply Chain Management sei definiert als die „innerbetrieblich und entlang der Lieferkette auch zwischenbetrieblich die auf das Gesamtsystem ausgerichtete strategische Koordinierung zwischen den traditionellen Geschäftsfunktionen [...] mit dem Ziel zur Verbesserung der langfristigen Leistungsfähigkeit der einzelnen Unternehmen und der Lieferkette als Ganzes.“[22] Aufgrund von vielen Verarbeitungsschritten, bevor ein Produkt den Konsumenten erreicht, können globale Lieferketten heutzutage hoch komplex sein und viele Parteien involvieren. Automatisierungen können zur Verbesserung von Prozessen in Lieferketten beitragen, beispielsweise geschieht die Verfolgung von Materialfluss und Produktionsschritten heutzutage häufig immernoch manuell. So sind Frachtbriefe ein hoher bürokratischer Aufwand, der in Lieferketten entsteht und kaum automatisiert ist.[23] Um dabei Regulierungen und Qualitätsstandards für Produkte einzuhalten, sind Transparenz und Nachverfolgbarkeit einzelner Produktionsschritte wichtig. Allerdings seien nach einer Befragung aus 2016 für nur 19 Prozent aus 1700 Unternehmen über die gesamte Lieferkette ihrer Produkte transparent informiert. 54 Prozent der Befragten hätten gar keine Transparenz in der Lieferkette. Produkthersteller seien dadurch in Ihrer Handlungsfähigkeit einge-

[21] Vgl. Baker et al. (2014): The Handbook of Logistics and Distribution Management: Understanding the Supply Chain S.5

[22] Vgl. Mentzer et al. (2001): Defining Supply Chain Management. Journal of Business Logistics S.22

[23] Vgl. Bosia, N et al. (2018): Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation S.64

schränkt, die Nachhaltigkeit ihrer Produkte zu verbessern.[24] So sollen offene und verteilte Blockchain Systeme neue Kollaborationsmöglichkeiten zwischen einzelnen Akteuren der Lieferkette ermöglichen und Prozesse automatisieren. Bis zu einem Drittel aller Prozesse üblicher Lieferketten seien durch die Implementierung offener verteilter Blockchain Systeme verbesserbar.[25] Eine Vielzahl von Projekten in Unternehmen forschen an der Implementierung von blockchainbasierten Lösungen zur effizienteren Kollaboration, der Optimierung von Bestandsführung und der Verbesserung von Anlagennutzung in Supply Chain Umgebungen. Jeder Produktionsschritt solle auf der Blockchain aufgezeichnet werden, sodass Kunden eine genaue und transparente Übersicht über Ihre Produkte erhalten.[26] Das Unternehmen Provenance beschreibt in ihrem Whitepaper einen auf der Blockchain-Technologie basierenden Lösungsansatz, der die Verfolgbarkeit von Zertifikaten und wichtigen Informationen aus Lieferketten ermöglichen solle. Physische Produkte seien digital repräsentierbar und nachweislich authentifizierbar. Ursprung und Herkunft seien auch für Kunden transparent nachverfolgbar.[27]

Sinn hierfür sei der Schutz vor gefälschten Gütern und dem mehrfachen Verwenden einmalig nutzbarer Zertifikate. Die Verifizierbarkeit von Zertifikaten sei heutzutage schwierig, aufwendig und kostspielig.

Argumentiert wird im Whitepaper, dass zentrale Systeme nicht transparent seien und somit Vertrauen eingeschränkt sei, weil diese für diskriminierendes Verhalten anfällig seien. Dabei solle die Blockchain als globales peer-to-peer Netzwerk eine offene Plattform bieten, die demgegenüber durch die technischen Architektur Neutralität, Verlässlichkeit und Sicherheit biete.

[24] Vgl. http://spendmatters.com/2016/04/27/consumer-goods-companies-lack-supply-chain-visibility-unable-to-assess-environmental-social-impacts-of-products/ [09.08.2019]

[25] Vgl. https://www.finextra.com/blogposting/12597/blockchain-in-the-supply-chain [09.08.2019]

[26] Vgl. https://cerasis.com/blockchain-in-supply-chain/ [09.08.2019]

[27] Vgl. https://www.provenance.org/whitepaper [13.08.2019]

Wird allerdings im Whitepaper nicht allzu tief auf die technische Umsetzung eingegangen, so wird noch von einem konsensbasierten, anreizstrukturbasierten Blockchain Datensystem gesprochen, die das Vertrauen einer zentralen Authorität obsolet mache. Transparent aufgezeichnet werden solle Zeit, das Produkt, die Quantität, Qualität und der aktuelle Besitzer. Jede Produktübergabe wird dann auf der Blockchain verfolgt und einsehbar. Anonymität sei für alle Rollen im System, wie dem Kunden oder dem Produzenten möglich, nur Zertifizierer müssen sich registrieren. Dabei hilft eine registrierende Authorität, jene verifiziert Identitäten der Zertifizierenden Parteien und zeichnet diese in der Blockchain auf. Produkte seien dann durch Tags mit der Blockchain verknüpft. Informationen können dann durch das Scannen des Tags auf den Produkten gelesen und von Nutzern mit entsprechenden Rechten veränderbar.

Sei einerseits von Neutralität des Systems die Rede, sprich der Obsoletmachung von Vertrauen an potenziell diskriminierende Institutionen, widerspricht sich dies allerdings mit der Tatsache, dass einerseits immernoch Vertrauen gegenüber den zertifizierenden Akteuren gegeben sein muss und denen, die die Registrierungen der Zertifizier verifizieren. Unerklärt bleibt, wie man als Produzent sensible Daten unveröffentlicht lassen kann. Werden alle Produktmengen und Schritte öffentlich gespeichert, wären sensible Produktionsvolumina und kritische Informationen über den gesamten Produktionsvorgang auch für die Konkurrenz einsehbar. Weiterhin muss vertraut werden, dass sich der aktuelle Zustand der Produkte tatsächlich in der Blockchain wiederspiegelt. Solle beispielsweise die Temperatur eines Produkts über einen Sensor überwacht werden, beispielsweise in gekühlten Produkten, so kann eine Blockchain nicht zur Sicherstellung jener Tatsache beisteuern, wenn der Fahrer den Sensor in einen kleinen Kühlschrank legt, nicht aber die eigentliche Lieferung, um Kosten zu sparen. Wird die Teilnahme an der Lieferkette durch bestimmte Parteien reguliert, so ist fragwürdig, warum

eine kostenaufwendige, teure Erhaltung von Dezentralität zwischen bekannten Parteien durch komplexe Proof-of-Work Verfahren nötig ist. Nach einer repräsentativen Befragung von 514 Logistik Unternehmen vom Bitkom Research habe jedes zweite Unternehmen im elektronische Frachtbegleitdokumente im innerdeutschen Einsatz.[28] Nach HGB § 408 Absatz 3 seien elektronische Frachtbriefe im innerdeutschen Einsatz dem analogen Frachtbrief gleichgestellt, allerdings seien im grenzübergreifenden Straßengüterverkehr CRM-Frachtbriefe immernoch gesetzliche Pflicht.[29]

5 Zusammenfassung

Das Verwenden einer Blockchain garantiert nicht, dass die Daten richtig eingetragen wurden. Dass die Daten der Realität entsprechen. Das Verwenden einer Blockchain ist per se keine Garantie für die Zuverlässigkeit der zu speichernden Daten, sondern eher hilfreich zur Konsistenz- erhaltung und Sicherheitserhaltung eines konsensbasierten, dezentralisierten Netzwerks. Vertrauen und Transparenz sind keine inhärente Eigenschaft von Blockchain Datenstrukturen. Allerdings können Vertrauen und Transparenz von verteilten Systemen durch den Zusammenschluss einer Blockchain, einem Proof-of-Work Konsensalgorithmus mit der Investition von extrinsischer Energie und intrinsischer spieltheoretischer Anreizstrukturen eine Dezentralisierung so massiv voranbringen, dass ein Potenzial zu Vertrauen, Transparenz und Zensurresistenz entstehen. Die Verwendung dieser Technologien sind gegenüber gebräuchlicheren Datenbankstrukturen mit einem immensen Mehraufwand und einer hohen Komplexität verbunden. Zentralisierte Software Lö-

[28] https://www.bitkom.org/Presse/Presseinformation/Logistik-muss-Digitalisierung-weiter-beschleunigen [19.08.2019]

[29] mm-logistik.vogel.de/papierlos-in-die-zukunft-digitale-dokumente-im-strassengueterverkehr-a-603606/ [19.08.2019]

sungen bieten performantere und einfachere Lösungswege und sollten daher zuerst in Erwägung gezogen werden. Außerhalb von frühen Ansätzen für Kryptowährungen gibt es zur Zeit noch keine funktionierende dezentralisierte Anwendung von offenen Blockchain Systeme. Die Vorstellung, dass durch die Verfügbarkeit einer neuen Technologie gesamte wirtschaftliche Prozesse dezentralisiert werden können, sollte kritisch reflektiert werden.

Literaturverzeichnis

[1] Baker, P. & Croucher, P. & Rushton, A. & Miller, A. & Goldfeder S. (2014) The Handbook of Logistics and Distribution Management: Understanding the Supply Chain 5th Ed., Kogan Page Limited

[2] Bonneau, J. & Felten, & E. Narayanan, A. (2016) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press

[3] Mentzer, J.T. & DeWitt, W. & Keebler, J.S. & Min, S. & Nix, N.W. & Smith, C.D. & Zacharia, Z.G. (2001) Defining Supply Chain Management, Journal of Business Logistics

[4] Tanenbaum, A. & Van Steen, M. (2006) Distributed Systems: Princibles and Paradigms, Vrije Universiteit Amsterdam

[5] Vukolic , M. (2015) The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, IBM Research - Zurich

[6] Bosia, N & Strewe, U.M. & Hofmann E. (2018) Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation, Springer Verlag

[7] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/öffentlich sein oder ebenfalls eingeschränkt sein. [12.08.2019]

[8] https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains [08.08.2019]

[9] https://www.coindesk.com/bitcoin-and-blockchain-the-tangled-history-of-two-tech-buzzwords [08.08.2019]

[10] https://consensys.net/academy/blockchain-basics-book/principles-of-decentralization [08.08.2019]

[11] https://www.finextra.com/blogposting/12597/blockchain-in-the-supply-chain [09.08.2019]

[12] https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf [08.08.2019]

[13] https://markshirecrypto.com/cryptocurrency/the-five-pillars-of-cryptocurrency/

[14] https://medium.com/@shyamshankar/centralized-ledgers-vs-distributed-ledgers-layman-understanding-52449264ae23 [08.08.2019]

[15] https://media.consensys.net/blockchain-vs-distributed-ledger-technologies-1e0289a87b16 [08.08.2019]

[16] https://www.provenance.org/whitepaper [13.08.2019]

[17] https://en.wikipedia.org/wiki/Blockchain [09.08.2019]