



HOCHSCHULE OSNABRÜCK

UNIVERSITY OF APPLIED SCIENCES

Projektbericht für die QS Qualität und Sicherheit GmbH, Bonn

**Ermittlung der Potenziale von ausgewählten Distributed Ledger
Technologien (Blockchain) in der Agri-Food-Chain
am Beispiel des QS-Systems**

Prof. Dr. Karin Schnitker | Simone Kemper M.Sc.
Fakultät Agrarwissenschaften & Landschaftsarchitektur
Fachbereich Unternehmensführung
Oldenburger Landstraße 62 | 49090 Osnabrück

31. Oktober 2019

Inhaltsverzeichnis

Abbildungsverzeichnis	4
Tabellenverzeichnis	5
1 Blockchain-Technologie	6
1.1 Blockchain – Ein erster Überblick	6
1.1.1 Definition und Charakteristika der Blockchain-Technologie	6
1.1.2 Abgrenzung verschiedener Blockchain-Arten	9
1.1.3 Ursprünge der Blockchain-Technologie	11
1.2 Funktionsweisen von BCT	12
1.2.1 Kryptographische Hash-Funktionen	12
1.2.2 Digitale Signatur	13
1.2.3 Blockchain-Datenstruktur	15
1.2.4 Blockaufbau	16
1.2.5 Netztopologie	17
1.2.6 Distribuierte Konsensverfahren	18
1.2.7 Smart Contracts und Oracles	24
1.2.8 Decentralized Applications (DApps)	28
1.3 Technische Bewertung	29
1.3.1 Technische Grenzen und Herausforderungen von Blockchain	29
1.3.2 Heutige Grenzen und Herausforderungen von Blockchain-Technologie	32
1.3.3 Technische Chancen und Potenziale	34
1.3.4 Technische Weiterentwicklungen von Blockchain	35
2 Entwicklungen von BCT im Agri-Food-Sektor und Anwendungsfelder	37
2.1 Marktübersicht von Blockchain-Projekten im Agri-Food-Sektor	37
2.2 Clusterung bisheriger Anwendungsfälle mit Relevanz für Lebensmittellieferketten	43
2.2.1 Supply Chain Management	43
2.2.1.1 Aktuelle Problemstellungen	44
2.2.1.2 Lösungspotenziale und Anwendungsbeispiele	44
2.2.1.3 Herausforderungen von Blockchain im Supply Chain Management	50
2.2.2 Auditierung und Zertifizierung	50
2.2.2.1 Aktuelle Problemstellungen	50
2.2.2.2 Lösungspotenziale und Anwendungsbeispiele	52
2.2.2.3 Herausforderungen von Blockchain in der Auditierung und Zertifizierung	53
2.2.3 Internet der Dinge (IoT)	53
2.2.3.1 Aktuelle Problemstellungen	53
2.2.3.2 Lösungspotenziale und Anwendungsbeispiele	54
2.2.3.3 Herausforderungen von Blockchain in Verbindung mit IoT-Lösungen	56

3	Hypothesen zur Relevanz von Blockchain für Lieferkette-Akteure	57
3.1	H1: Form des Vertrauens in abgespeicherte Daten verändert sich durch Blockchain-Lösung	57
3.2	H2: Manipulationssicherheit der BCT kann besonders für Echtheitsnachweise im asiatischen Markt interessant werden/sein	59
3.3	H3: Hype um Blockchain unter Lebensmittelhändlern liegt im Interesse an maximaler Transparenz der Zulieferströme	60
3.4	H4: Blockchain dient in diversen Projekten eher als Marketinginstrument	61
3.5	H5: Eigenschaften der Blockchain kann Unternehmen / Branchen vor Reputationsschäden besser schützen	62
4	Hypothesen zur Relevanz von Blockchain für QS als Standardgeber.....	63
4.1	H1: Zentrale, unabhängige Kontrollinstanzen wird es auch in einer „Blockchain-Lieferkette“ bedürfen	63
4.2	H2: Blockchain könnte zu einem Paradigmenwechsel hinsichtlich des Eigentums an Daten im QS-System führen.....	65
4.3	H3: Blockchain-Technologie als Katalysator für IoT und Big Data könnte künftig die Art und Weise von Audits verändern.....	65
4.4	H4: Derzeitige Blockchain-Entwicklungen im Handel könnten u. U. zu einer stärkeren Verhandlungsmacht des LEHs ggü. Zulieferern und auch dem QS-System führen	66
5	Kritische Würdigung der Methoden und Ergebnisse, Fazit und Ausblick	68
5.1	Kritische Würdigung der Methoden und Ergebnisse	68
5.2	Fazit und Handlungsempfehlungen	69
Anhang.....		73
Literaturverzeichnis		78

Abbildungsverzeichnis

Abb. 1:	Ausprägungen der Blockchain-Technologie (i. A. an Meinel et al. 2018).....	11
Abb. 2:	Technische Elemente der Blockchain-Technologie (eigene Darstellung)	12
Abb. 3:	Verwendung asymmetrischer Schlüsselpaare (Hinckeldeyn 2019)	14
Abb. 4:	Blockaufbau und -struktur (eigene Darstellung)	15
Abb. 5:	Merkle Tree (Antonopoulos 2017).....	16
Abb. 6:	Unterschiede de-/zentraler und verteilter Netzwerktopologie (Swanson 2015)....	18
Abb. 7:	Komplexitätsgrad von Smart Contracts (Morrison 2016)	26
Abb. 8:	Agri-Food-Akteure mit Blockchain-Pilotprojekten (eigene Darstellung)	38
Abb. 9:	Bereits relevante Akteure für den Ag/Food-Bereich im Blockchain-Ecosystem ...	40
Abb. 10:	Agri-Food-Blockchainprojekte von 2016 bis 2019 (i.A. an Anhang 1).....	42
Abb. 11:	Sawtooth für Seafood Supply Chain Traceability (Hyperledger Sawtooth 2018) .	56
Abb. 12:	Ebenen der Vertrauensbildung (Düring et al. 2017, S. 452)	58
Abb. 13:	Entscheidungsbaum für Verwendung von Blockchain (i. A. an Peck 2017; Kückelhaus et al. 2018; Meunier 2018)	71

Tabellenverzeichnis

Tab. 1:	Differenzierung des Blockchain-Begriffes (Burgwinkel 2016; Swan 2015)	7
Tab. 2:	Merkmale verschiedener Blockchain-Ausprägungen (i. A. an Drescher 2017)	11
Tab. 3:	Abgrenzung möglicher Netzwerkstrukturen (Swanson 2015; Burgwinkel 2016) ..	18
Tab. 4:	Gegenüberstellung vorgestellter Konsensmodelle (Bogensperger et al. 2018) ...	24
Tab. 5:	Ausprägungen von Smart Contract Oracles.....	27
Tab. 6:	Vor- und Nachteile von Smart Contracts für BCT.....	27
Tab. 7:	Module des IBM Food Trust Systems (IBM Food Trust 2019).....	48
Tab. 8:	Stärken, Schwächen, Chancen und Risiken der Blockchain-Technologie.....	69

1 Blockchain-Technologie

1.1 Blockchain – Ein erster Überblick

Im folgenden Abschnitt wird ein Überblick der wesentlichen Funktionsweisen sowie technischen Grundlagen von Blockchain-Technologie (BCT) gegeben. Neben einer Begriffsdefinition und -abgrenzung werden unterschiedliche Ausprägungen der BCT dargestellt. Das Kapitel schließt mit einer Darstellung der Ursprünge dieser Enabler-Technologie ab.

1.1.1 Definition und Charakteristika der Blockchain-Technologie

Nach (Mattila 2016) oder (Swan 2015) lässt sich der Terminus Blockchain heute noch nicht einheitlich definieren. Die Betrachtung diverser Publikationen, die sich mit der Definition von BCT auseinandersetzen, zeigt aber dennoch wesentliche Gemeinsamkeiten, mit denen die Technologie beschrieben werden kann. So kann eine Blockchain **als digitales Protokoll oder Register** verstanden werden, indem Transaktionen, Ereignisinformationen oder sonstige Daten in einem **dezentralen Netzwerk** durch die Netzwerkteilnehmer verwaltet werden (Condos et al. 2016). Dabei werden **Informationen „blockweise“ verarbeitet** und **chronologisch** mittels kryptographischer Signaturen miteinander zu einer „Kette“ verknüpft (Walport 2015). Aus den Definitionen der zitierten Autoren wird deutlich, dass sich *die* Blockchain als elektronisches Kontenbuch oder Register von der dahinterstehenden Verwaltungssystematik der BCT unterscheidet. Glaser und Bezenberger (2015) definieren die Blockchain-Technologie als einen dezentralen Konsensmechanismus, der auf Elementen der **Kryptographie** und **Peer-to-Peer-Logik (P2P) aufbaut** und so ein digitales Verwaltungssystem für manipulationssichere Daten ermöglicht. Anstelle einer einzigen zentralen, autoritären Kontrollinstanz werden neue Informationen im Netzwerk durch einen Konsens der Netzwerkteilnehmer selbst verifiziert (Schlatt et al. 2016). Hosp (2018) gibt folgende zusammenfassende Definition:

*„Eine Blockchain ist eine digitale Datei, in der dieselbe Information von allen Mitgliedern einer Gesellschaft abgespeichert und Updates in regelmäßigen Zeitblöcken an die bereits bestehende Information gehängt werden, sodass jeder Teilnehmer die gesamte Information besitzt und **sich nicht auf andere verlassen muss.**“*

Die wesentlichen Elemente der BCT – Kryptographie und Dezentralität – in Form von P2P-Netzwerken werden nachfolgend näher erläutert: Nach Mullender (1995) lassen sich dezentrale Datenbanksysteme nicht eindeutig definieren und lediglich anhand diverser Charaktereigenschaften identifizieren. Entscheidend ist nach Schlatt et al. (2016) die Vernetzung räumlich verteilter, voneinander unabhängiger Rechner bzw. Netzwerkknoten zur Kommunikation und kontinuierlichen Synchronisation des aktuellen, replizierten

Informationsstatus. Bei einem Ausfall eines Rechners bzw. Knotenpunktes arbeitet das übrige Netzwerk ohne Beeinträchtigung weiter, sobald der ausgefallene Knotenpunkt wieder online im Netzwerk ist, aktualisiert sich seine gespeicherte Version der Blockchain auf den aktuellen Informationsstatus. Bezeichnend für ein Peer-to-Peer-Netzwerk ist zudem die bereits erwähnte, **direkte Interaktion** von Teilnehmern bzw. Knotenpunkten beim Austausch von Daten, ohne dass es einer zentralen Koordinations- / Kontrollinstanz bedarf (Schoder und Fischbach 2002; Glaser und Bezenberger 2015).

Bei der ersten Blockchain-Anwendung ‚Bitcoin‘ werden alle Transaktionsdaten aus einem Zeitfenster von zehn Minuten erfasst und als Block der bestehenden Blockchain angehängen. Auf diese Weise entsteht eine chronologische und lineare Aneinanderreihung von Datenblöcken. Jeder neu angefügte Block beinhaltet einen Referenzwert zu seinem Vorgängerblock, wodurch die Verkettung der einzelnen Blöcke entsteht. Als Full Nodes bezeichnete Rechner im Netzwerk, realisieren dank ihrer ausreichenden Rechenleistung das sog. Mining. Neben der gesamten Blockchain haben diese Rechner bzw. ihrer Betreiber eine zusätzliche Mining-Applikation lokal installiert, um die Generierung neuer Blöcke und die Verifizierung eingehender Transaktionen sicherzustellen (Swan 2015; Burgwinkel 2016).

In der bestehenden Fachliteratur werden verschiedene Blockchain-Begriffe teilweise unter dem Oberbegriff „Blockchain“ angeführt. In der nachfolgende Tabellen 1 werden BCT-Begriffe differenziert, die oftmals fälschlicherweise unter dem identischen Oberbegriff gemeint sind:

Tab. 1: Differenzierung des Blockchain-Begriffes (Burgwinkel 2016; Swan 2015)

Begriff	Definition
Blockchain als Architektur	Gemeint ist die Kombination verschiedener Disziplinen der Informationstechnologie: Verschlüsselung mittels Hash-Algorithmus – z. B. SHA256 und der Nutzung einer digitalen Signatur bzw. asymmetrischer Schlüsselpaare.
Blockchain-Plattformen	Gemeint ist das verteilte Netzwerk – bestehend aus über das Internet miteinander verbundenen, voneinander unabhängigen Rechnern – in denen die Blockchain-Software genutzt wird.
Blockchain-Software	Gemeint ist der Programmcode, der notwendig ist, um im Netzwerk auch tatsächlich agieren zu können. Bereits 2016 sind nach (Burgwinkel) über 20 Software-Lösungen (Open-Source und Kommerziell) vorhanden. Als Beispiele sind hier die Software von ‚Bitcoin‘ oder ‚Ethereum‘ zu nennen.
Blockchain-Applikation	Applikationen werden auf Basis der Software auf einer Blockchain Plattform angeboten. Bsp.: Auf der Ethereum-Software können mehrere Applikationen realisiert werden (IDEX oder EtherDelta).
Blockchain 1.0	Die Anwendung von Blockchain in der ersten Generation bezog sich ausschließlich auf Kryptowährungen und den digitalen Zahlungsverkehr
Blockchain 2.0	In der zweiten Generation von Blockchain-Anwendungen wurden mittels der Realisierung von Smart Contracts Geschäftsprozesse, die über eine Finanztransaktion hinausgehen, auf Basis einer Blockchain-Software abbildbar.

Blockchain 3.0	In der dritten Generation dehnt sich die Anwendung von Blockchain auf sämtliche Wirtschaftsbereiche (Behörden, Gesundheitssystem etc.) aus.
Blockchain-as-a-Service (BaaS)	Blockchain als Service auf Basis einer Cloud-Lösung, wobei aber alle beschriebenen Ebenen berücksichtigt sind.

Zusammenfassend lassen sich an dieser Stelle bereits die wesentlichen Charaktereigenschaften von Blockchain Technologie festhalten. Neben den Grundprinzipien der Technologie, die bereits im ersten White Paper zu Blockchain bei Nakamoto (2009) inbegriffen waren, sind im Laufe der Entwicklung noch weitere Eigenschaften hinzugekommen. Heute finden sich diese Grundprinzipien jeweils unterschiedlich ausgeprägt immer wieder. Nachfolgend werden diese in Kürze dargestellt (Tanenbaum und van Steen 2016; Mougayar und Buterin 2016; Tapscott und Tapscott 2018).

Blockchain als verteiltes Netzwerk, das offen zugänglich ist und einen direkten Austausch zwischen den Netzwerkteilnehmern erlaubt:

1. Es bedarf keines Vertrauensintermediärs, da das System ohne Vertrauen zwischen den Teilnehmern funktioniert.
2. Einmal abgespeicherte Informationen in der „*Blockkette*“ sind nachträglich unveränderbar.
3. Die Blockchain Technologie kennzeichnet sich durch ihre Sicherheit, die auf den Grundsätzen der Kryptographie basiert. Auf diese Weise ist zudem die anonyme Interaktion im Netzwerk abbildbar.

Bedingt durch die Entwicklung hin zur zweiten Generation der Blockchain Technologie und die Umsetzung von Smart Contracts sind weitere Charakteristika hinzugekommen (Swan 2015):

4. Automatisierung von Geschäftsbedingungen / -prozessen.
5. Interaktion im Rahmen einer Transaktion auf beliebige Prozessschritte ausdehnbar.

Des Weiteren ist die Technologie in Bezug auf den Kontext unterschiedlich zu betrachten. Mougayar und Buterin (2016) grenzen hier drei Dimensionen voneinander ab:

1. Technische Sichtweise = Blockchain als Datenbank-System im Backend, auf dessen Basis die Verwaltung eines digitalen, offenen Ledgers abbildbar ist.
2. Wirtschaftliche Sichtweise = Blockchain als Netzwerk, das den digitalen und direkten Austausch von Werten zwischen seinen Systemteilnehmern ermöglicht.

3. Rechtliche Sichtweise = Blockchain als Prinzip bzw. Verfahren um vertrauensbedürftige Transaktionsprozesse digital ohne einen Intermediär abzubilden.

1.1.2 Abgrenzung verschiedener Blockchain-Arten

Eine Blockchain kann in verschiedenen Ausprägungen genutzt werden. Je nach Anforderungen der Netzwerkteilnehmer lässt sich das Protokoll der zu nutzenden Blockchain-Lösung entsprechend formulieren. Grundsätzlich lassen sich die unterschiedlichen Blockchain-Arten anhand von zwei Eigenschaften voneinander abgrenzen: (1) den Zugriffsrechten und (2) der Konsenslogik (Drescher 2017).

Bei den Zugriffsrechten unterscheidet man zwischen sog. **Private** und **Public Blockchains**:

Bei einer **öffentlichen (public) Blockchain** kann jeder durch den Download des Codes am Netzwerk teilnehmen und einen Knotenpunkt betreiben. Handelt es sich dabei um eine sog. **Permissionless Blockchain in Bezug auf die angewandte Konsenslogik**, kann außerdem jeder Teilnehmer des Netzwerkes am Validierungsprozess neuer Transaktionen mitwirken. Eine solche Blockchain steht also grundsätzlich jedermann für weltweite Transaktionen offen. Transaktionen sind damit vollkommen transparent, aber dennoch anonym, da jeder Teilnehmer unter einem „Pseudonym“ – in Form seines öffentlichen Schlüssels – im Netzwerk agiert. Beispiele für diese Blockchain-Form sind die ‚Bitcoin‘-Blockchain, ‚Ethereum‘, ‚Litecoin‘ oder ‚Dash‘. Die wesentliche Motivation bei einer solchen Ausprägung liegt in dem Misstrauen ggü. zentralen Kontrollinstanzen. Den größten Einfluss kann diese Form von Blockchain daher auf die Disruption bestehender Geschäftsmodelle nehmen, die als Intermediäre zwischen den eigentlichen Geschäftspartnern agieren. Durch die absolute Dezentralität des Netzwerkes, verteilt auf die Rechner der Teilnehmer, minimieren sich zudem die Infrastrukturkosten, da kein großer Hauptserver gewartet und betrieben werden muss bzw. vor einem Ausfall oder Hacker-Angriffen aufwendig geschützt werden muss (Drescher 2017; Meinel et al. 2018).

Konsortiale, Federated Blockchains: Im Gegensatz zu öffentlichen, permissionless Blockchains, wie z. B. der ‚Bitcoin‘-Blockchain, werden konsortiale Blockchains von einer Gruppe von Unternehmen oder anderen Institutionen geführt bzw. betrieben. Diese Form der Blockchain kann hinsichtlich der Lese- und Schreibrechte für jedermann frei zugänglich sein oder den Mitgliedern des Konsortiums vorbehalten sein. Die Validierung neuer Transaktionen obliegt aber vorab definierten Knotenpunkten, die i. d. R. verteilt bei den Mitgliedern des Konsortiums liegen. Durch die geringere Anzahl an Knotenpunkten, die am Konsensprozess teilnehmen, liegt bei dieser Blockchain-Form eine höhere Skalierbarkeit vor. Transaktionen können somit schneller durchgeführt werden (Hosp 2018). Beispiele für konsortiale Blockchain-Lösungen finden sich im Bankensektor, der Energie- oder Logistikbranche: 20

Institutionen schließen sich zusammen, um eine branchenfähige Blockchain-Lösung zu realisieren und betreiben dazu jeweils einen Knotenpunkt für die Validierung von Transaktionen. Als Beispiele für diese Form der Blockchain-Technologie sind ‚r3‘, ‚Corda‘, ‚EWF‘ (Energie) oder ‚B3i‘ (Versicherungen) zu nennen. Den größten Einfluss hat diese Ausprägung der BCT auf das Potenzial der Transaktionskostenreduktion, indem Dokumentations- und Compliance-Aufwand minimiert werden können (Meinel et al. 2018). Diese Form der BCT kann damit grundsätzlich als weniger disruptiv eingestuft werden, als die Public Blockchains. Die möglichen Kosten- und Effizienzvorteile im Business-Kontext sind aber nichtsdestotrotz zu bedenken (Meinel et al. 2018; Hosp 2018)

Private Blockchains umfassen Anwendungen der Blockchain-Technologie in einem einander bekannten Teilnehmerkreis, zwar mit verteilten Speichermedium, aber bspw. innerhalb eines Unternehmens oder einer Institution.

Bei dieser Ausprägung der BCT geht der eigentliche Mehrwert der Disintermediation verloren. So obliegen die Schreibrechte und der Konsensprozess zur Validierung neuer Transaktionsinformationen einer klar definierten Gruppe an Teilnehmern, die i. d. R. einer einzigen Organisation angehören. Leserechte können in einem solchen Fall öffentlich oder zumindest einer breiteren Anzahl an Nutzern erteilt werden. Während Skalierbarkeit und Datenschutz in solchen Blockchain-Lösungen ggü. öffentlichen BCs optimiert sind, liegt das Problem in der Vertrauenswürdigkeit der prüfenden Teilnehmer, die eher zentralen Charakter haben. Denkbar sind solche Anwendungen für Datenmanagement oder Auditprozesse innerhalb eines Unternehmens oder einer Organisation. Ein Beispiel für diese Ausprägung von BCT ist ‚MultiChain‘ (Meinel et al. 2018).

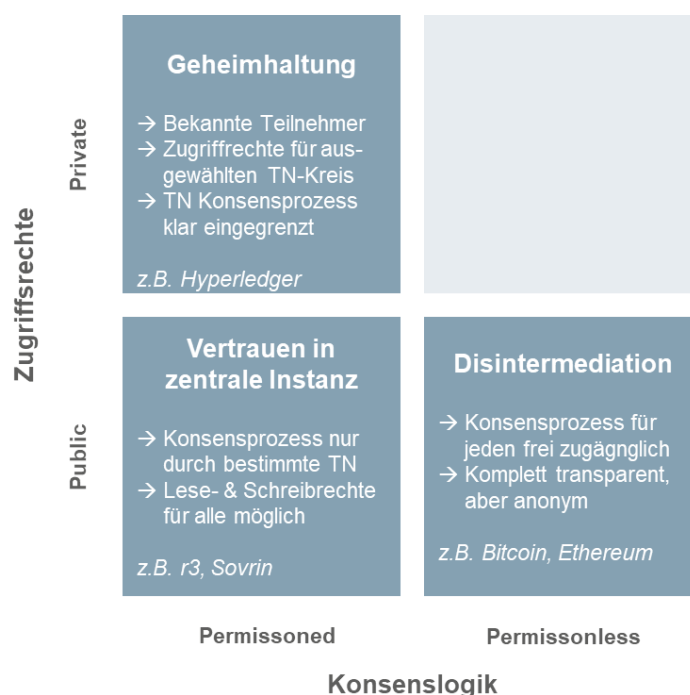


Abb. 1: Ausprägungen der Blockchain-Technologie (i. A. an Meinel et al. 2018)

Der Unterschied bzw. die Vorteile zwischen privaten und öffentlichen Blockchains lässt sich anhand der folgenden Merkmale verdeutlichen:

Tab. 2: Merkmale verschiedener Blockchain-Ausprägungen (i. A. an Drescher 2017)

	PUBLIC	PRIVATE, KONSORTIAL
Zugang	Frei zugänglich	Berechtigung für Schreib- und Leserechte nötig
Geschwindigkeit zur Verifizierung	Langsamer	Schneller
Sicherheit	Proof of Work, Proof of Stake, weitere Konsensmechanismen für Validierung	Wahlen oder Multi-Party-Consensus Algorithmus
Identität	Anonym bzw. Pseudonym	Akteure eindeutig identifizierbar
Impact	Disruptiv für Intermediäre	Reduktion von Transaktionskosten, Steigerung der Transparenz oder Minimierung von Datenreduanzen

1.1.3 Ursprünge der Blockchain-Technologie

Um Blockchain zu begreifen, hilft es einen Blick auf die Entstehung der ersten Blockchain-Anwendung ‚Bitcoin‘ zu werfen: Zu unterscheiden sind die beiden Begriffe relativ leicht. So ist ‚Bitcoin‘ eine Anwendung der Blockchain-Technologie. Man kann sich vorstellen, dass Blockchain wie ein Betriebssystem vorhanden sein muss, um diverse Anwendungen nutzen zu können. Bitcoin ist dabei nur eine von vielen Anwendungen, die auf Basis von Blockchain realisierbar ist. Die Entwicklung der Blockchain-Technologie geht dabei in der Geschichte der Informatik weit zurück. Als ersten Ansatzpunkt kann die Erfindung von Ralph Merkle im Jahr 1979 mit dem Merkle-Tree-Prinzip genannt werden. Die erste elektronische Währung wurde 1983 von David Chaum in einem White Paper diskutiert. In den 1990er-Jahre wurde erstmalig die kryptographische Verkettung einzelner Datensätze mittels Hash-Blöcken entwickelt (Bayer et al. 1993). Adam Back stellte 1997 die Basis eines Algorithmus vor, der das Proof-of-Work-Prinzip¹ von Bitcoin darstellte und damit die Grundvoraussetzung digitaler Währungen darstellt. Ursprünglich wurde Proof-of-Work entwickelt, um E-Mail-Spams entgegenzuwirken. Aus einer Kombination all dieser Ansätze ist Blockchain entstanden. Die ursprüngliche Idee dieser Technologie wird im Whitepaper von Bitcoin (2008) beschrieben: Auslöser waren Vertrauensverluste in zentrale Institutionen, die mit ihnen anvertrauten monetären Werten risikoreiche Geschäfte tätigten. Vertrauensmissbrauch und damit einhergehender Datenmissbrauch hatten globale Auswirkungen auf Wirtschaftssysteme. Die Idee hinter der Blockchain-Technologie war eine Veränderung auf systemischer Ebene, um Veruntreuung /

¹ Proof-of-Work ist das derzeit bekannteste Konsensverfahren in der Blockchain-Technologie und dient dazu, in einem dezentralen System ohne „die eine“ Kontrollinstanz Einigkeit unter den Teilnehmern über Wahrheitszustände zu definieren. Nähere Erläuterung in [Kapitel 1.2.6](#)

Betrug digital zu erschweren und zentrale Kontrolleinheiten mit einer ungleichen Machtverteilung in einem System überflüssig zu machen (Antonopoulos 2018; Rosenberger 2018).

1.2 Funktionsweisen von BCT

Um die Funktionsweisen der Blockchain Technologie zu verstehen und nachzuvollziehen, warum die o. g. Charaktereigenschaften der Technologie überhaupt möglich sind, hilft ein grundsätzliches Verständnis der Einzelelemente, die innerhalb der BCT ihre Anwendung finden. Aus technischer Sicht liegt die Innovation der BCT in der einzigartigen Kombination aus Elementen der Informatik zu einem kohärenten Ansatz, wie es ihn vorher eben nicht gab. Die nachfolgende Abbildung fasst diese Elemente zusammen, auf die im Nachgang jeweils in Kürze eingegangen wird.



Abb. 2: Technische Elemente der Blockchain-Technologie (eigene Darstellung)

1.2.1 Kryptographische Hash-Funktionen

Eine Hash-Funktion ermöglicht die Verschlüsselung eines beliebig langen Inputwertes zu einer immer einheitlich langen Abfolge von hexadezimalen Zeichen, die als Hashwert bezeichnet wird. Verändert man die ursprüngliche Zeichenfolge nur minimal, so ändert sich der daraus resultierende Hash-Wert gravierend (Condos et al. 2016; Franco 2014). Hashfunktionen reduzieren damit große Datenmengen in eine kleinere Zeichenfolge und können als der digitale Fingerabdruck eines Datensatzes verstanden werden, über den ein Datensatz eindeutig identifiziert werden kann (Gupta 2017; Hinckeldeyn 2019). In der Blockchain-Technologie wird derzeit der Secure Hash Algorithm SHA-256 verwendet. Die Zahl 256 gibt dabei an, dass ein Hash-Wert immer eine Größe von 256 Bit besitzt. Diese Hash-Funktion gilt bis heute als extrem sicher hinsichtlich der Verschlüsselung von Datensätzen (Narayanan et al. 2016).

Grundsätzlich lassen sich **fünf Eigenschaften** der kryptographischen Hashfunktionen zusammenfassen (Drescher 2017):

Zuerst sind kryptographische Hashfunktionen **kollisionsresistent**. Mit einer Kollision ist gemeint, dass aus zwei unterschiedlichen, voneinander unabhängigen Inputgrößen der gleiche Hashwert resultiert. Kollisionsresistenz besteht demnach, wenn kein identischer Hashwert für zwei voneinander abweichende Inputdaten generiert wird (Hinckeldeyn 2019). Aus mathematischer Sicht kann es zwar theoretisch zu einer solchen Kollision kommen, praktisch benötigt ein Rechner, der 10.000 Hash-Werte/Sek. berechnen kann, bei einer SHA256-Hashfunktion über 10^{27} Jahre, um lediglich die Hälfte aller Kombinationsmöglichkeiten auf eine Hash-Kollision zu prüfen (Paar et al. 2010).

Dennoch sind die Hashwerte dabei **deterministisch**, d. h. eine Hashfunktion generiert bei identischem Dateninput immer wieder exakt den gleichen Hashwert. Die dritte Eigenschaft liegt in der **Pseudozufälligkeit** der generierten Hashwerte. Dies bedeutet, dass eine minimale Änderung bei der Dateneingabe zu einem völlig anderen Hashwert führt.

Bei kryptographischen Hashfunktionen handelt es sich zudem um sog. **Einwegfunktionen** (Hinckeldeyn 2019). Bekannt unter dem Begriff **Nonce** (Number only used once), wird dem Inputdatensatz eine beliebige, geheime Zahl beigefügt. Mittels dieses Nonce lässt sich ein Inputwert nachträglich nicht mehr einfach so ermitteln (Bogensperger et al. 2018).

Die fünfte Eigenschaft von Hash-Funktionen ist die sog. **Puzzle Friendliness**. Mathematisch beschrieben liegt hierin die Tatsache, dass ein Nonce-Wert in einer Hash-Funktion für jede Outputmöglichkeit n der Funktion nicht unterhalb der Zeit 2^n gefunden werden kann. Diese Eigenschaft führt dazu, dass sich keine Lösungsstrategie besser empfiehlt als das schiere Durchprobieren von möglichen Nonce-Werten, bis der richtige Nonce-Wert gefunden wurde (Adolph et al. 2019).

Für die Blockchain-Technologie stellen kryptographische Hashfunktionen ein wesentliches Element dar. So lassen sich auf diese Weise Transaktionsdaten verschlüsseln, eindeutig identifizieren und verifizieren sowie signieren. Nach Wang et al. (2019) lassen sich generell sechs Anwendungen von Hashfunktionen in der Blockchain-Technologie kategorisieren:

- Hiding-Prozess: Transaktionsdaten mit Zufallszahlen versehen
- Verteilte Konsensmechanismen (siehe Kap. 1.2.6)
- Signaturen bei Transaktionsdurchführung (siehe Kap. 1.2.2)
- Identitätsnachweise
- Blockgenerierung (siehe 1.2.3)
- Adresserstellung für Blockchain-Anwendungen

1.2.2 Digitale Signatur

Das **Prinzip der Digitalen Signaturen** ist in der Kryptographie schon in den 1970er Jahren diskutiert worden und auf Diffie und Hellman (1976) zurückzuführen (Schlatt et al. 2016). Mit

der Generierung eines asymmetrischen, mathematisch miteinander verbundenen Schlüsselpaares (je ein privater und ein öffentlicher Schlüssel) können digitale Signaturen erstellt werden (Franco 2014). Hierbei werden Hashwerte auf Basis von Sicherheitswerten erzeugt. Jeder Netzwerkteilnehmer erhält ein asymmetrisches Schlüsselpaar: der private Schlüssel muss dabei geheim bleiben, der öffentliche Schlüssel wird dem Netzwerk vorgestellt (Hinckeldeyn 2019). Während der Ersteller einer Nachricht mit seinem privaten Schlüssel „unterschreibt“, sendet er die signierte Botschaft an den öffentlichen Schlüssel des Empfängers. Der Empfänger wiederum kann die Nachricht nun mit dem öffentlichen Schlüssel des Absenders abgleichen und so auf Authentizität überprüfen (Diffie und Hellman 1976). Entschlüsselt wird die Nachricht wiederum mit dem privaten Schlüssel des Empfängers. Auf diese Weise liefert die digitale Signatur für jeden Teilnehmer im Netzwerk eine Identität. So lassen sich Aktionen im Netzwerk personalisieren und Signaturen nicht replizieren (Narayanan et al. 2016). Mit dieser Funktionsweise erfüllt die sog. Public-Key-Kryptographie zwei wesentliche Anforderungen an die Blockchain-Technologie: die sichere Datenübertragung im Netzwerk und die eindeutige Identifikation von Netzwerkteilnehmern – zwar unter Pseudonym, aber unverfälschbar und sicher (Schlatt et al. 2016). Die nachfolgende Abbildung von Hinckeldeyn (2019) veranschaulicht die Verwendung in der Blockchain-Technologie:

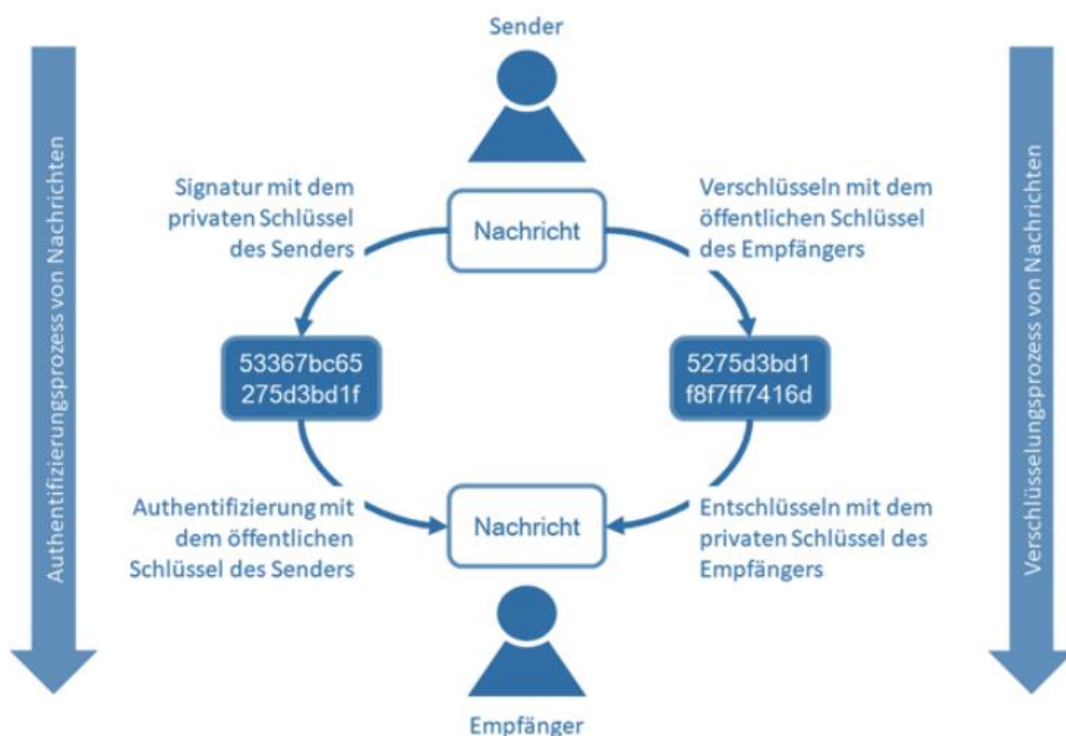


Abb. 3: Verwendung asymmetrischer Schlüsselpaare (Hinckeldeyn 2019)

1.2.3 Blockchain-Datenstruktur

Die mittels Hash-Funktion verschlüsselten Datensätze gilt es in einem strukturierten Verfahren abzulegen. Dabei ist nicht nur der Dateninhalt selbst, sondern auch die Signatur und die Verknüpfung der einzelnen Blöcke zueinander berücksichtigt. Zur Verknüpfung der Blöcke dient der sog. Hash-Pointer, welcher eine Referenz zu seinem Vorgänger-Block umfasst und damit die im Vorgängerblock berechneten Datensätze berücksichtigt. Verändert sich ein Wert in einem Vorgängerblock, passt der Hash-Pointer des Folgeblocks nicht mehr und ab dieser Stelle ist die gesamte Kette in ihren Hash-Pointern nicht mehr in sich stringent. Ziel der Hash-Pointer ist damit in erster Linie, die Manipulationssicherheit einer Blockchain zu realisieren. Die nachfolgende Abbildung 4 veranschaulicht die Struktur der Blöcke. Im der unteren Kette werden dabei die Folgen eines Manipulationsversuchs veranschaulicht: Ändert sich ein Hashwert einer Transaktion in Block 2, ändert sich der Hash-Pointer dieses Blocks, sodass dieser nicht mehr mit den Daten in Block 3 übereinstimmt.



Abb. 4: Blockaufbau und -struktur (eigene Darstellung)

Neben den essentiellen Angaben in der Abbildung 4, die für die Verkettung der einzelnen Blöcke wichtig sind, werden noch weitere Angaben in einem jeden Block hinterlegt. Auf diese wird im nachfolgenden Kapitel 1.2.4 noch weiter eingegangen. Zuvor wird in Kürze die Datenstruktur zur Verknüpfung einzelner Blöcke in einer Blockchain erläutert.

Merkle Tree: Eine effiziente Datenstruktur, die mithilfe von Hash-Pointern möglich wird, ist der sog. Merkle Tree. Mittels baumartiger Datenstruktur können umfassendere Datenmengen effizient zusammengefasst, verifiziert und hinsichtlich ihrer Integrität kontrolliert werden. (Antonopoulos 2017) zeigt die typische Struktur mit folgender Abbildung 5.

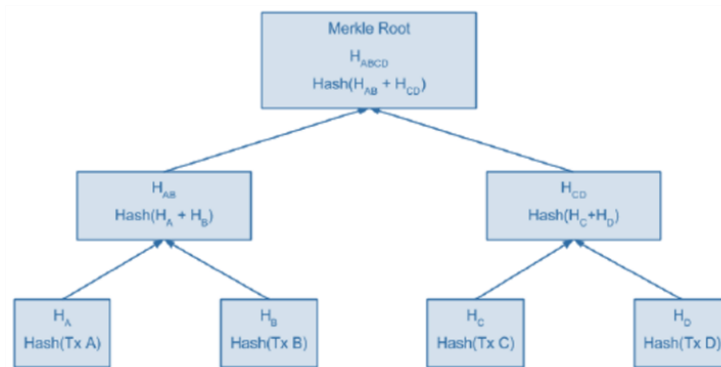


Abb. 5: Merkle Tree (Antonopoulos 2017)

In dieser Datenstruktur werden jeweils zwei Blöcke zusammengefasst, die zwei Hashwerte beinhalten (H_A und H_B). Ziel einer solchen Datenstruktur ist es, mehrere Transaktionen unter einem Hashwert zu gruppieren. Dazu werden kontinuierlich auf jeder Ebene zwei Hashwerte addiert, bis nur noch ein einziger Hashwert übrig bleibt. Diesen bezeichnet man als den sog. Merkle Root (Buchmann et al. 2007). Wird nun einer der Werte manipuliert, wirkt sich dies auf den gesamten Pfad bis zum Merkle Root aus, sodass eine Manipulation schnell erkannt und deren Quelle identifiziert werden kann (Merkle 1990).

1.2.4 Blockaufbau

Die Blockchain baut sich aus chronologisch aneinandergereihten Blöcken auf, in denen jeweils die ausgeführten Transaktionsinformationen zu einer Anwendung in einer Blockchain-Software liegen. Ein Block kann also als Speicher von Transaktionen verstanden werden (Antonopoulos 2017).

Abbildung 4 zeigt bereits den groben Aufbau eines Blocks, mit der Unterteilung in den sog. Block Header und den Datenbereich. Im Block Header, also dem „Blockkopf“, sind die nötigen Informationen zur Verknüpfung der Einzelblöcke mit der bestehenden Blockchain und zum Konsensmechanismus aufgeführt. Die Identität des Blocks – bezeichnet als sog. Header Hash, also der Hash-Wert dieses Blocks – wird zusammen mit dem Previous Hash, also dem Hashwert des Vorgängerblocks im Block Header abgelegt. Mittels Zeitstempel, dem sog. Timestamp liegt in diesem Teil zudem die Information darüber, wann der Block erstellt wurde. Ein sog. Difficulty Wert gibt Hinweis auf den Schwierigkeitsgrad im Konsensprozess. Der bereits erwähnte Nonce Wert, welcher bereits im Abschnitt zur kryptographischen Hashfunktion erläutert wurde, ist ebenfalls im Block Header angelegt. Wird sich der üblichen Datenstruktur des Merkle Tree bedient, liegt im Header zudem der sog. Merkle Root, also der Hashwert des obersten Blocks im Merkle Tree (Antonopoulos 2017).

Im Datenbereich eines Blocks liegen währenddessen Transaktionsinformationen, bei denen üblicherweise der Übergang von Tokens oder Coins von einem Netzwerkteilnehmer zum

anderen dokumentiert ist. An dieser Stelle sind die Begriffe Coin und Token in Kürze voneinander abzugrenzen:

Als einen Coin bezeichnet man im Blockchain-Kontext den Träger eines fix definierten Wertes, bspw. ein Bitcoin. Als Token bezeichnet man hingegen die technische Weiterentwicklung von Coins. Auch ein Token gilt als Träger eines Wertes, dieser Wert kann jedoch mehrdimensionale Informationen enthalten. Ein Token ist damit mehr als eine Währung, er ist eher als kryptographisch-verifizierter Beleg für einen Zustand im Netzwerk zu verstehen. Bekanntestes Beispiel für einen Token ist ein ‚Smart Contract‘² (Swanson 2015).

1.2.5 Netztopologie

Weitere Charaktereigenschaft und Funktionsweise der Blockchain Technologie ist die verteilte Netzwerkstruktur, bei der es sich um sog. Peer-to-Peer-Netzwerke handelt. Unter einem Peer-to-Peer Netzwerk versteht man ein selbstorganisiertes System mit unabhängigen, autonomen Rechneinheiten (Peers), die Informationen im Netzwerk unmittelbar miteinander teilen können, ohne dass es einer zentralen Serviceinstanz bedarf (Oram 2001).

Auf Basis dieser typischen Netztopologie der Blockchain Technologie sollte nach Burgwinkel (2016) korrekterweise von einem verteilten System gesprochen werden. Wobei sich das P2P-Netzwerk in einer Blockchain von einem reinen P2P-Netzwerk durch einen relevanten Aspekt unterscheidet: Die Blockchain als Datensatz ist weder an einem zentralen Ort im Netzwerk, noch fragmentiert auf den Knotenpunkten des P2P-Systems gespeichert. Auf unterschiedlichen Knotenpunkten liegt hingegen jeweils eine vollständige Kopie der gesamten Daten, abgespeichert in der oben beschriebenen Datenstruktur. Findet nun auf einem Knotenpunkt ein Manipulationsversuch statt, kann in der Kopie auf dem betroffenen Knotenpunkt ein gültiger Hash-Wert vorliegen, dieser wird sich aber nun nicht mehr mit den Replikaten der Blockchain auf allen anderen Knotenpunkten decken. Swanson (2015) grenzt die Unterschiede eines reinen P2P-Netzwerkes (dezentrales Netzwerk) und eines verteilten Blockchain-Netzwerkes mit folgender Abbildung voneinander ab.

² Smart Contracts sind „selbstausführende“ Verträge, die auf Computerprotokollen basieren. Sie bauen auf der Blockchain-Technologie auf und ermöglichen eine automatisierte Prüfung von Bedingungen zwischen zwei Vertragspartnern sowie entsprechende Auslösung von Aktionen, auf Grundlage entsprechender Bedingungen. Nähere Erläuterung zu Smart Contracts unter [Kap. 1.2.7](#)



Abb. 6: Unterschiede de-/zentraler und verteilter Netzwerktopologie (Swanson 2015)

Die nachfolgende Tabelle fasst die wesentlichen Unterschiede dieser drei Netzwerktopologien abschließend zusammen:

Tab. 3: Abgrenzung möglicher Netzwerkstrukturen (Swanson 2015; Burgwinkel 2016)

	Zentral	Dezentral	Verteilt
Fehleranfälligkeit	hohe Anfälligkeit, da Totalausfall möglich	bedingte Anfälligkeit, da mit Directory Peer ganze Netz-werkteile wegfallen können → System beschränkt nutzbar	kein Systemausfall möglich, da alle Peers gesamtes System stützen können.
Wartung	Simple Wartung, da nur eine zentrale Einheit betroffen ist	Aufwendiger, da mehrere Points of Failure beachtet werden müssen	Schwierige Wartung, da alle Peers involviert sind
Aufbauaufwand	Gering, da zentrale Abstimmung	Langsam, da Standards abzustimmen sind	Langsam, da Standards abzustimmen sind
Entscheidungsprinzip	Zentral, hierarchisch	Gleichberechtigung auf lokalen Informationsständen	Autonome, verteilt koordinierte Prozesse
Diversität	Gering, da zentraler Frame	Hohe Diversität führt zu schneller Weiterentwicklung	Hohe Diversität führt zu schneller Weiterentwicklung
Geschwindigkeit	Je nach Leistung der zentralen Einheit	Je nach Leistung des adressierten Peers	Langsam, da Verarbeitung über jeden Peer erfolgen kann

1.2.6 Distribuierte Konsensverfahren

Eine der Kernfunktionen der Blockchain-Technologie ist die Anwendung von Konsensmechanismen, mit denen eine P2P-Interaktion von Werten in einem Netzwerk ohne vertrauensgebende Instanz erst möglich wird. Dabei wird das Protokoll, welches den Konsens in einem Netzwerk herstellt, als sog. Konsensalgorithmus betitelt. Die Idee des digitalen Austauschs von Werten kursierte schon lange vor der ersten Anwendung von Blockchain.

Dabei stellten sich aber zwei Probleme, die ohne Konsensalgorithmus zuvor nicht lösbar waren. Erstens, das sog. Double Spending, also die Möglichkeit, eine Währungseinheit bzw. ein digitales Asset zeitgleich an zwei Adressen zu versenden und damit doppelt auszugeben. Und Zweitens das sog. „Problem der Byzantinischen Generäle“ (siehe Folgeabschnitt). Die Blockchain-Technologie löst beide Probleme durch die „zeitdiskrete“ und auf viele Knotenpunkte verteilte Validierung von Transaktionen. Damit ist an dieser Stelle bereits festzuhalten, dass erst durch die Konsensverfahren die Möglichkeit der sicheren Interaktion im Netzwerk gegeben ist. Darüber hinaus bezwecken sie die notwendige Einigung über den jeweils nächsten Block, der an die bestehende Blockchain angehängt werden soll (Walport 2015; Voshmgir 2016).

Bevor die relevantesten Konsensverfahren vorgestellt werden, gibt der nächste Abschnitt einen kurzen Überblick über das Problem der byzantinischen Generäle, um die Bedeutung der Konsensverfahren besser nachvollziehen zu können:

Die Analogie der byzantinischen Generäle beschreibt die Herausforderung, in einem verteilten Netzwerk mit Teilnehmern, die einander nicht vertrauen, einen Konsens herzustellen. Man stelle sich eine Belagerung mehrerer Armeen, mit jeweils einem General vor. Die Armeen sind räumlich voneinander getrennt, sodass die Generäle nur über Nachrichten kommunizieren können. Eine Eroberung kann nur dann erfolgreich sein, wenn alle Generäle zeitgleich bzw. abgestimmt angreifen. Das Problem liegt hier zum einen in der Übermittlung der Botschaften mittels Boten. Kann diesen und den übertragenen Botschaften vertraut werden? Und ein zweites Problem liegt in der Vertrauenswürdigkeit der Generäle selbst. So könnte einer der Generäle ein Betrüger sein. Sobald ein Konsensalgorithmus dieses Problem der mangelnden Vertrauenswürdigkeit räumlich getrennter Instanzen lösen kann und ein Anteil an Betrügern dem Konsens des Systems nicht schaden kann, spricht man von einer „byzantine fault tolerance“ im Blockchain-Netzwerk (Hinckeldeyn 2019).

Mittlerweile haben sich verschiedene Konsens-Ansätze für Blockchain-Plattformen entwickelt, die je nach Systemanforderung vorteilhafter sein können (Voshmgir 2016). Die derzeit relevantesten Konsensverfahren werden nachfolgend näher erläutert.

Proof-of-Work (PoW) ist das derzeit bekannteste Konsensmodell und hat im Rahmen des Whitepapers zu Bitcoin von Satoshi Nakamoto die Grundlage für die Realisierung von Blockchain-Technologie erst ermöglicht (Nakamoto 2009). Die Idee des PoW-Ansatzes liegt darin, dass Netzwerkteilnehmer, die am Konsensprozess teilnehmen wollen (sog. Miner) zueinander in Wettbewerb treten und ihren Arbeitsaufwand in einem solchen Konsensprozess, in Form von Rechenleistung (Hashing Power) nachweisen. Dabei ist für die Validierung eines jeden neuen Blocks ein kryptographisches Rätsel von den Minern zu lösen. Die konkreten

Schritte für die mathematische Berechnung des kryptographischen Rätsels ist z. B. Bogensperger et al. (2018) zu entnehmen.

Als Vorteile des PoW-Ansatzes lässt sich grundsätzlich festhalten, dass heute ein hohes Maß an Vertrauen in diese Form der Konsensmechanismen herrscht, da zahlreiche Blockchain-Implementierungen erfolgreich mit dem PoW-Konsensmodell arbeiten. Gerade bei offenen Netzwerken, wie bei Kryptowährungen, bringt PoW eine vorteilhafte Skalierbarkeit. So funktioniert der Konsensmechanismus ohne die Authentifizierung der Teilnehmer und kann beliebig viele Knotenpunkte umfassen. Für eine Manipulation im Validierungsprozess benötigt ein Betrüger min. 50 Prozent der insgesamt verfügbaren Rechenleistung des kompletten Netzwerks. Auch wenn dies theoretisch möglich wäre, lohnt es sich bisher wirtschaftlich nicht. Experten betiteln den PoW-Ansatz zudem als den „fairsten“ Ansatz der Konsensmechanismen, da der Aufwand eines Miners entsprechend entlohnt wird (Buntinx 2017).

Massiver Nachteil dieses Konsensverfahrens wird von verschiedensten Autoren angeführt und bezieht sich auf den hohen Stromverbrauch, der durch die nötige Rechnerleistung entsteht. Hinzukommt die Kritik an der theoretischen Manipulierbarkeit des Validierungsprozesses bei einem 51 %-Anteil der Gesamtrechenleistung des Netzwerkes. Auch wenn es sich heute praktisch noch nicht lohnt, ist diese theoretische Sicherheitslücke des Konsensmechanismus mit Blick auf Quantencomputer usw. als wesentlicher Nachteil zu berücksichtigen (Vries 2018). Vergleicht man die Validierungszeit in einem Blockchain-Netzwerk auf PoW-Basis mit der Validierungszeit bzw. Transaktionszeiten von VISA oder MasterCard, liegt ein wesentlicher Nachteil des PoW-Verfahrens in der Anzahl an möglichen Transaktionen je Sekunde im Netzwerk. Zur Lösung dieses Problems wird aktuell an verschiedenen Ansätzen geforscht (Strüker 2017; Baliga 2017).

Für ‚Ethereum‘ hat sich ein spezieller PoW-Konsens entwickelt, der sog. Ethash. Wesentliches Merkmal liegt in der deutlich kürzeren Zeitspanne je Block von nur noch 12-19 Sekunden und dem verstärkten Vorgehen gegen eine Mining-Zentralisierung und damit verbundene 51%-Angriffe. So kann Ethash auf standardmäßiger Endverbraucher-Hardware durchgeführt werden. Patentierte Hardware schützt ergänzend vor einer konzentrierten Hashing-Power (Baliga 2017).

Proof-of-Stake (PoS) seit 2011 kursiert dieses Konsensverfahren als relevanteste Alternative zum PoW-Ansatz in der Blockchain-Community (Bogensperger et al. 2018). Primär soll mit diesem Verfahren dem massiven Stromverbrauch des PoW entgegengewirkt werden. Dabei wird hinsichtlich der Terminologie nicht mehr von „Minern“, sondern von „Validatoren“ gesprochen, die den Konsensprozess im Netzwerk umsetzen und dabei den Miningprozess in erster Linie „virtueller“ abbilden als im PoW-Verfahren. Die Entschädigung der Validatoren für

ihre Aufwendungen im Konsensprozess erfolgt dabei durch Transaktionsentgelte. Während sich die Miner im PoW-Prozess mit ihrer Hardware (also Rechnerleistung) höhere Chancen im Wettbewerb zu anderen Minern verschaffen, wird im PoS-Verfahren mit Wertanteilen im System gearbeitet. Dazu stellen die Validatoren ihr Vermögen innerhalb des Netzwerkes als Pfand zur Verfügung. Brechen sie die definierten Konsensregeln, so erhalten sie den Pfand nicht zurück und verlieren ihr Vermögen (Bogensperger et al. 2018).

Grundidee des PoS-Verfahrens ist damit also die „Virtualisierung“ des Miningprozesses. Anstelle der Investition in Hardware und Stromverbrauch, kann ein Netzwerkteilnehmer in die Kryptowährung des Blockchain-Systems investieren und sich so Anteile (Stakes) sichern. Proportional zu seinen Einlageanteilen steigt auch seine Chance als Validator für einen neuen Block ausgewählt zu werden und die entsprechenden Transaktionsentgelte des Blocks als Gegenleistung zu erhalten (Drescher 2017). Versucht der ausgewählte Validator bei der Blockerstellung zu betrügen, würde der ungültige Block auffallen und der Sicherheitspfand des Validators erlöschen. Seine Möglichkeit, damit am Konsensverfahren im Netzwerk teilzunehmen, wäre damit ebenfalls hinfällig. Während kein Validator aufgrund eines sog. Pseudozufallsalgorithmus vorhersehen kann, ob er beim nächsten Block ausgewählt wird, kann die Berechnung des kryptographischen Rätsels, welche zur Blockerstellung nötig ist, wesentlich einfacher sein als beim PoW. Auf diese Weise sinkt der Energieverbrauch im Vergleich zum PoW-Verfahren deutlich herab. Zusammenfassend ist der PoS-Ansatz mit einem ökonomischen Lotteriespiel zu vergleichen: Jeder kann am Konsensverfahren als Validator teilnehmen, sofern er über eine Anteilseinlage (Coins) verfügt, die als Pfand für ein korrektes Verhalten im Falle einer Blockerstellung dient. Auf diese Weise wird im PoS-Verfahren fehlerfreies Verhalten der Teilnehmer durch deren Kapitalbeteiligung erzielt (Mougaray und Buterin 2016).

Die Auswahl eines Validators für die Erstellung eines neuen Blocks kann dabei auf unterschiedliche Art und Weise erfolgen. Wie bereits oben erläutert, besteht grundsätzlich die Möglichkeit der komplett randomisierten Auswahl des Knotenpunktes, der den nächsten Block erstellt. In dieser Auswahlvariante sind die Einlagen der einzelnen Knotenpunkte öffentlich einsehbar. Damit ist eine Abschätzung der wahrscheinlichsten Knotenpunkte, die ausgewählt werden könnten, grundsätzlich abbildbar. Ein zweites Auswahlverfahren ist auf Basis des Alters von Coins möglich, die ein Teilnehmer besitzt. Das Coin-Alter errechnet sich aus dem Zeitraum seiner Entstehung multipliziert mit seinem Wert. Daraus resultiert im PoS-Verfahren: Je länger ein Netzwerkteilnehmer seine Coins besitzt, desto höher sind seine Rechte, die er im System hält (Whitepaper NXT 2018).

Wie bereits genannt, liegt ein wesentlicher Vorteil des PoS in der Reduktion des Stromverbrauchs und damit einhergehenden Reduktion der Transaktionskosten. Zudem

schaft die Virtualisierung und Ökonomisierung des Miningprozesses eine erhöhte Sicherheit für das Netzwerk. Ein manipulierender Player müsste mit 51 % aller Coins zuerst die Marktmacht erlangen. Darauf würde das System während der Übernahme von Anteilen bereits mit Preiserhöhungen reagieren. Ist ein Player doch in Besitz von über 50 % aller Einlagen, würde ein Angriff ihn selbst am stärksten treffen, sodass diese Sicherheitslücke im Grunde einen wirtschaftlichen Widerspruch darstellt (Drescher 2017).

Darüber hinaus ermöglicht der PoS-Ansatz kürzere Blockzeiten und entsprechend eine Erhöhung der Transaktionsraten. Hinzu kommt der Vorteil, dass mit dem bestehenden Kapitalbestand des Systems flexibler agiert werden kann, da keine kontinuierliche Schaffung neuer Coins als Anreiz für die Miner nötig ist. Die Virtualisierung des Miningprozesses führt zudem zu einer stärkeren Streuung an Netzwerkknoten, die sich am Konsens beteiligen, da die Zugangsbarrieren und die notwendigen Hardware-Voraussetzungen im Vergleich zu PoW deutlich reduziert sind. Somit wird auch der Gefahr der Zentralisierung entgegengewirkt (Antonopoulos 2018).

Als Nachteile des PoS-Mechanismus werden grundsätzlich drei Punkte angeführt. So funktioniert ein solches System nur dann, wenn auch ein Bestrafungsmechanismus für fehlerhaftes Verhalten integriert ist. Des Weiteren sind Wallets³ mit einem hohen Anteil an Coins, die jederzeit online sind, vor Angriffen gefährdet. Dritter, oft angeführter Nachteil des PoS liegt in der Tatsache, dass ein proportionales Verhältnis zwischen der Rendite aus der Konsensprozess-Teilnahme und den Anteilen im Netzwerk herrscht. Dies kann makroökonomisch zu einer steigenden Konzentration des Systemkapitals führen (Bogensperger et al. 2018).

Proof-of-Authority (PoA) ist das Konsensverfahren, welches permissioned Blockchains ausmacht. Hierbei erfolgt vor der Teilnahme am Konsensmechanismus im Netzwerk zuerst eine Autorisierung der Validatoren. Es kann also im Gegensatz zum PoS und PoW nicht einfach jeder Knotenpunkt am Konsensverfahren teilnehmen, sondern unter einer ausgewählten Anzahl an Knotenpunkten wird der Konsens Block für Block eruiert. Daher wird beim PoA auch von sog. Authorities gesprochen, denen das Recht der Validierung neuer Blöcke vorbehalten ist. Mithilfe sog. rundenbasierter Algorithmen wird hierbei für jede „Runde“ einer der Authority-Knotenpunkte ernannt, der die Rolle des sog. „Mining leaders“ einnimmt und neue Blockvorschläge in das System gibt. Um einen verteilten Konsens zu erreichen, muss der überwiegende Anteil an Authorities die Gültigkeit des entstehenden Blocks bestätigen und dafür Rechenschaft ablegen. Aufgrund dieser Funktionsweisen empfiehlt sich

³ Als Wallet wird im Blockchain-Kontext ein digitales Bankkonto eines Nutzers bezeichnet. Über ein sog. Wallet können Nutzer Transaktionen untereinander tätigen. Über ein Wallet werden Zugangsschlüssel für das Auslösen von Transaktionen eines Teilnehmers gespeichert.

der PoA für private bzw. konsortiale Blockchain-Lösungen. So nutzen bspw. Blockchain-Lösungen, wie ‚Hyperledger‘ oder ‚Ripple‘ diese Art des Konsensmechanismus oder auch permissioned Blockchain-Ansätze auf Basis von ‚Ethereum‘ (Angelis et al. 2017; Prusty 2017).

Wesentliche Vorteile von PoA liegen in der geringeren Ressourcenaufwendung im Vergleich zu PoW und der besseren Leistungsfähigkeit verglichen mit dem PoS-Verfahren, da ein Mining-Prozess im engeren Sinne nicht mehr nötig ist. Verglichen mit der Funktionsweise zentraler Datenbanken liefert der PoA-Ansatz eine Möglichkeit, private bzw. konsortiale Netzwerke sicherer ggü. Angreifern zu machen. So kann ein Angreifer nie ein komplettes Netzwerk einnehmen oder alle bestehenden Transaktionen manipulieren bzw. löschen (Bogensperger et al. 2018).

Als Nachteil wird hierbei jedoch der Verlust der eigentlichen Grundidee von Blockchain kritisiert, da eine tatsächliche Dezentralität und Demokratisierung von Netzwerken – wie es in öffentlichen Blockchains der Fall ist – mit diesem Konsensverfahren nicht abbildbar ist. Die Macht bzw. das Vertrauen im korrekten Validieren neuer Datensätze liegt bei ausgewählten, autorisierten Knotenpunkten des Netzwerks (Meinel et al. 2018). Im Gegensatz zentralen Lösungen (z.B. das klassische Online-Banking) erlaubt der PoA-Mechanismus aber dennoch ein **verteiltes** Verfahren zur Verifizierung von Datensätzen.

Practical Byzantine Fault Tolerance (PBFT) ist ein weiterer Konsensmechanismus, der v.a. mit Blick auf private Blockchain-Lösungen beachtenswert ist. Auf Basis des Problems der byzantinischen Generäle wurde dieser Konsensalgorithmus von (Castro und Liskov 1999) vorgestellt. Dabei existiert im Netzwerk ebenfalls eine ausgewählte Gruppe von Validatoren, um eingehende Transaktionen der übrigen Netzwerkteilnehmer (Clients) auf Gültigkeit zu prüfen. Der Unterschied liegt in der Ernennung eines bestimmten Validators, der per Zufall bei jeder Transaktion ausgewählt wird (Leader). Nur an den Leader wird die Transaktion gesendet und dieser gibt sie an die übrigen Validatoren weiter. Diese senden wiederum eine Zustimmung an den ursprünglichen Auftraggeber (Client). Sobald der Client von min. 2/3 aller Validatoren eine Zustimmung erhalten hat, gilt die Transaktion als ausgeführt.

Der Vorteil dieses Konsensverfahrens liegt in der Effizienz hinsichtlich des Durchsatzes an Transaktionen und dem geringen Energiebedarf. Zusätzlich sind einmal angenommene Transaktionen in diesem System final und lassen sich nicht, wie im PoW-Verfahren, nachträglich theoretisch doch noch unter hohem Aufwand manipulieren. Als nachteilig wird allerdings der immense Kommunikationsaufwand im System angesehen, der proportional mit der Anzahl an Netzwerkteilnehmern ansteigt. Dieses Verfahren eignet sich daher primär für kleinere Netzwerke (Castro und Liskov 1999; Hinckeldeyn 2019).

Die nachfolgende Tabelle fasst die wesentlichen Merkmale der vier vorgestellten Konsensverfahren abschließend zusammen.

Tab. 4: Gegenüberstellung vorgestellter Konsensmodelle (Bogensperger et al. 2018)

	PoW	PoS	PoA	PBFT
Teilnahme-möglichkeit	offen	offen	beschränkt	beschränkt
Energiebedarf	hoch	mittel	niedrig	niedrig
Transaktions-rate	gering	hoch	hoch	sehr hoch
Manipulations-toleranz	min. 51 % der Gesamt-rechenleistung	min. 51 % des Gesamt-kapitals	min. 33 % der Stimmrechte	max. 33 % fehlerhafte Kopien
Skalierbarkeit Netzwerk-volumen	hoch	hoch	gering	gering
Beispiel-anwendung	Bitcoin	2019: Umstellung von Ethereum	Microsoft Azure, Ethereum Private	Hyperledger Fabric

1.2.7 Smart Contracts und Oracles

Nach Wright und Filippi (2015) bestand die Idee von Smart Contracts bereits 1996 mit einer Publikation von NICK SZABO. Aber erst mit der BCT besteht nun erstmalig ein Katalysator für Smart Contracts, da so erst die dezentrale Abbildung ohne vertrauensgebenden Intermediär möglich wird (DeRose 2016; Wright und Filippi 2015; Schlatt et al. 2016). In Verbindung mit der BCT tauchten Smart Contracts erstmalig im Ethereum White Paper im Jahr 2014 auf. Smart Contracts sind als Codes oder Programme zu verstehen, die Vertragsbedingungen (vergleichbar mit WENN-DANN-Funktionen) enthalten. Die Erweiterung der Blockchain-Technologie um die Anwendung von Smart Contracts hat im Wesentlichen zur Evolution von Blockchain 1.0 zu 2.0 beigetragen. Basierend auf externem Informationsinput (sog. Information Oracles) können Smart Contracts dann **automatisierte Aktionen** ausführen und **miteinander interagieren**, nach vorab definierten Netzwerkregeln (Tuesta et al. 2015). Bedingungen und daraus resultierende Aktionen können dabei einen hohen Komplexitätsgrad erreichen und komplette Geschäftsprozesse automatisiert abbilden. Als Teil eines Blockchain-Netzwerkes agiert ein Smart Contract ähnlich einem Netzwerkteilnehmer mit einem Public Key, niemand besitzt jedoch den dazugehörigen Private Key. Ist ein Smart Contract einmal erstellt, lassen sich dessen Inhalte nicht mehr verändern. Das Konto des Smart Contracts führt nun die ihm vorgeschriebenen Aktionen je nach Erfüllung der gegebenen Bedingungen aus (Swan 2015).

Die Nutzenpotenziale von Smart Contracts liegen in erster Linie in der automatisierten Speicherung und Verwaltung von Daten sowie der Möglichkeit, Daten für andere Smart Contracts zur Verfügung zu stellen. Wesentliche Anwendung von Smart Contracts liegt aber in der Verwaltung von Vertragsbeziehungen zwischen einander unbekanntem Netzwerkteilnehmern, ohne dass es eine zentrale Vertrauensinstanz bedarf. Aber auch für die Erstellung von Tokens und in Authentifizierungsprozesse kommen Smart Contracts zum Einsatz (Bogensperger et al. 2018; Buterin 2014). Swanson (2014) sieht damit in Smart Contracts ein elementares Hilfsmittel, um bisher menschlich gesteuerte Vertragsgebaren zu automatisieren und Vertragserfüllung und Vertragsstrafen bzw. Sanktionen abbilden zu können. Anwendungspotenziale für Smart Contracts werden vor diesem Hintergrund in verschiedenen Geschäftsmodellen gesehen. Gerade in Kombination mit IoT⁴-Anwendungen wird ein großes Potenzial gesehen. So können bspw. bei Mietmodellen zeitweise Zugangsberechtigungen an smarten Türschlössern ohne Ausstellung eines physischen Schlüssels realisiert werden (Schlatt et al. 2016).

Beispiel Mietwagen-Nutzung mit Smart Contracts und IoT-Lösung (Schlatt et al. 2016)

Ein digitaler Autoschlüssel wird über die Blockchain erst dann an den Nutzer freigeschaltet, wenn dieser die Bezahlung für den Mietwagen veranlasst hat. Nach Ablauf der Mietdauer wird dem Nutzer der Zugang automatisch wieder entzogen. Sobald also ein Ereignis mit direktem Bezug zu den Vertragsinhalten eintritt, wird über einen in die Blockchain geschriebenes Programm (Smart Contract) eine Handlungsaktion ausgelöst. Kautionsrückzahlungen oder der Einbehalt der Kautions bei Beschwerde des nachfolgenden Nutzers, Zugangsberechtigungen und Bezahlprozess können dabei unveränderbar, transparent und dennoch so anonym wie notwendig über eine Blockchain abgebildet werden.

Weitere Anwendungsfelder von Smart Contracts erstrecken sich von der Versicherungswirtschaft über die Energiebranche bis hin zu dezentralen, autonomen Organisationen (DAOs). Der Komplexitätsgrad intelligenter Verträge ist theoretisch von technischer Seite aus unbegrenzt, sodass ganze Organisationen dezentral und autonom auf diese Weise agieren könnten. Herausforderungen liegen aber in der Umsetzung und

⁴ Vom Internet of Things (IoT) spricht man, wenn mehr als Laptop und Smart Phone mit dem Internet verbunden sind. Quasi jedes Gerät im Haushalt oder Produktionsmaschinen könnten sich mit dem Internet verbinden und so untereinander kommunizieren (Hosp 2018).

Bsp. Die smarte Kaffeemaschine erkennt, wenn Bohnen zur Neige gehen und prüft über ein smartes Lagerregal, ob im Vorrat noch Bohnen verfügbar sind. Falls nicht, bestellt sie selbst bspw. via Amazon Fresh neue Bohnen.

möglichen Plausibilitätswidernsprüchen in den einzelnen Funktionen. Die nachfolgende Abbildung von Morrison (2016) veranschaulicht die verschiedenen Anwendungsgebiete von Smart Contracts mit steigendem Komplexitätsgrad.

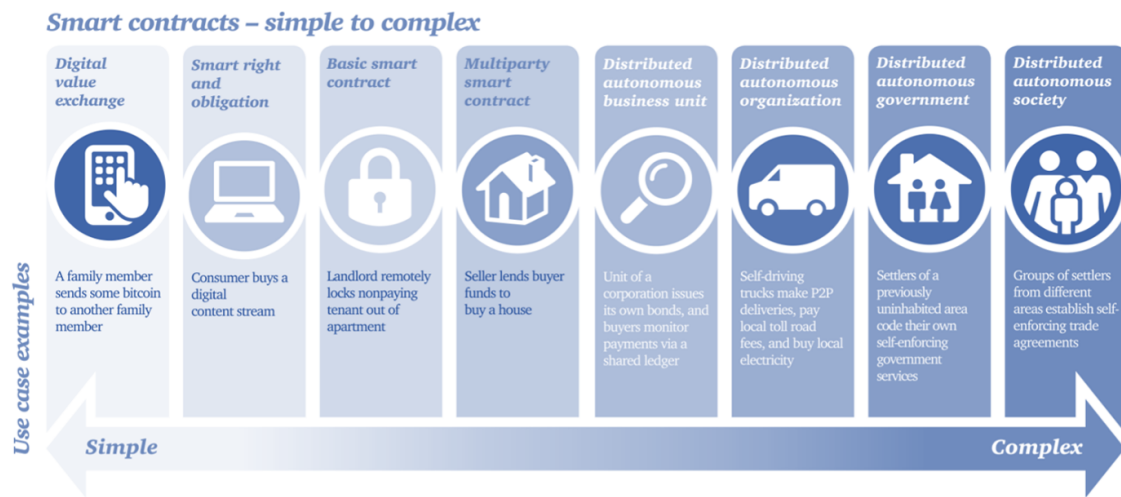


Abb. 7: Komplexitätsgrad von Smart Contracts (Morrison 2016)

Zusammenfassend lässt sich festhalten, dass durch Smart Contracts Vertragserfüllungen bzw. -bedingungen quasi in Echtzeit geprüft werden können und definierte Folgebedingungen automatisiert ausgeführt werden können. Smart Contracts besitzen also die Charaktereigenschaften „**Selbstüberprüfend**“ sowie „**Selbstaufführend**“ und sind aufgrund der BCT zudem **manipulationssicher**. Damit lassen sich bspw. gesetzliche Vorgaben oder Standardanforderungen automatisiert nachvollziehen und reduzieren so auch die Notwendigkeit eines unabhängigen Intermediärs, wodurch Transaktionskosten optimiert werden können (Bogensperger et al. 2018).

Eine Weiterentwicklung des grundsätzlichen Smart Contracts stellen die sog. ‚Smart Contract Oracles‘ dar. Durch diesen Ansatz wird die Verknüpfung zwischen Blockchain-Welt und externer Welt möglich, indem die Interaktion mit Systemen außerhalb der Blockchain abbildbar ist. Smart Contract Oracles können dabei in zwei Richtungen zwischen Blockchain-Plattform und Außenwelt agieren. So ermöglichen sie einerseits den Input externer Dateninformationen oder Ereignisse innerhalb der Blockchain, um entsprechende Aktionen eines Smart Contracts auszuführen. Oracles funktionieren aber auch in die Gegenrichtung, um Aktionen außerhalb des Blockchain-Netzwerks auszuführen. Damit ergibt sich bspw. die Möglichkeit, verschiedene Blockchain-Netzwerke miteinander zu verbinden. So erlaubt z. B. ein Oracle auf der Ethereum-Plattform das Auslösen einer Transaktion innerhalb der Bitcoin-Blockchain. Die o.g. inputorientierte Oracle-Form erlaubt die Integration von externen Daten, die bereits auf digitalen Plattformen (z. B. SAP, CRM, etc.) bestehen oder über Webseiten online sind. Realisierbar ist auch der Input über Sensoren aus der physischen Welt sowie die Integration

„echter“ Verträge, die nach elektronischer Unterschrift mittels Smart Contracts entsprechend ausgeführt werden (Tuesta et al. 2015).

Grundsätzlich werden fünf Arten von Smart Contract Oracles unterschieden, wie der nachfolgenden Tabelle zu entnehmen ist (Voshmgir 2016):

Tab. 5: Ausprägungen von Smart Contract Oracles

Software Oracle	<ul style="list-style-type: none"> ▪ Daten sind bereits online, bspw. auf Webseiten, z. B. Markt-, Mess-, Nutzungsdaten ▪ Oracle verarbeitet diese bereits verfügbaren Daten für einen Smart Contract
Hardware Oracle	<ul style="list-style-type: none"> ▪ Daten werden mittels Sensoren in der physischen Welt erfasst z. B. RFID-Chips, Temperatur- oder Feuchtigkeitssensoren
Inbound Oracle	<ul style="list-style-type: none"> ▪ Daten von externer Quelle liefern Input an Smart Contract, um Aktion auszuführen, z. B. Ausführung eines Kaufs, sobald ein handelbares Produkt eine Preisgrenze von X erreicht hat.
Outbound Oracle	<ul style="list-style-type: none"> ▪ Ausgabe von Smart Contract-Output in die Außenwelt z. B. autom. Öffnung eines Türschlosses, sobald eine Zahlung im Blockchain-Netzwerk erfolgt ist und bei der Netzwerkadresse eingegangen ist.
Consensus-based Oracle	<ul style="list-style-type: none"> ▪ Berücksichtigung von verschied. Datenquellen möglich z. B. relevant für Geschäftsprozesse auf Basis von Prognosen

Wie bereits zuvor erläutert, stellt die Anwendung von Smart Contracts und die Erweiterung um Oracles einen Evolutionsschritt in der Blockchain-Technologie dar. So bilden Smart Contracts letztlich den Dateninput von sog. DApps ab, die im folgenden Abschnitt näher erläutert werden. Vorab gibt die nachfolgende Tabelle jedoch abschließend eine Übersicht der Kernvor- sowie nachteile von Smart Contracts.

Tab. 6: Vor- und Nachteile von Smart Contracts für BCT

Vorteile	Nachteile
<ul style="list-style-type: none"> ▪ Automatisierte Ausführung von vorab definierten Bedingungen, ▪ ohne die Notwendigkeit eines Intermediärs, der die Bedingungen prüfen muss oder ggf. manipulieren kann (Juels et al. 2015). 	<ul style="list-style-type: none"> ▪ Vertragsbedingungen und daraus resultierende Folgeaktionen werden eingangs definiert und entsprechend programmiert. Die Ausführung erfolgt jedes Mal exakt so, wie dem Programm vorgegeben (Tuesta et al. 2015).
<ul style="list-style-type: none"> ▪ Echtzeit-Ausführung von Vertragsbedingungen wird möglich. 	<ul style="list-style-type: none"> ▪ Definitions- und Implementierungsphase ist damit bei komplexen Konstrukten extrem aufwendig.
<ul style="list-style-type: none"> ▪ Kostensenkung und Effizienzsteigerung für Vertragsdurchsetzung, Compliance und Interaktion der Vertragsparteien. 	<ul style="list-style-type: none"> ▪ Sollte trotz aufwendiger Implementierung ein Fehler im Programmcode enthalten sein, kann das dramatische wirtschaftliche Folgen haben.
<ul style="list-style-type: none"> ▪ Brücke in die externe, reale Welt wird so für BCT möglich. Smart Contracts + Oracles schaffen damit völlig neue Reichweite an Anwendungsfeldern f. BCT. 	<ul style="list-style-type: none"> ▪ Aktuell mangelt es noch an einer rechtlichen Basis für Smart Contracts und die Möglichkeit, sein Recht auf Basis entspr. Grundlagen geltend zu machen (Brown 2015).

1.2.8 Decentralized Applications (DApps)

Während Smart Contract Oracles die Schnittstelle zwischen Smart Contracts und Außenwelt herstellen, sind DApps die Schnittstelle von Nutzer zu Blockchain. Dabei handelt es sich um dezentral, im P2P-Netzwerk angelegte Software-Anwendungen, die es den Netzwerkteilnehmern ermöglichen, miteinander zu agieren. Grundsätzlich kann man DApps auch als „die Umsetzung von Geschäftsmodellen auf Basis einer (Blockchain-) P2P-Plattform“ verstehen (Bogensperger et al. 2018). Dabei stellt das Backend einer solchen DApp einen Smart Contract dar, der auf der Blockchain dezentral ausgeführt wird. Hierhin liegt der wesentliche Unterschied zu üblichen Anwendungen, die i. d. R. mittels Server oder Endgerät zentral ablaufen. Das Frontend (Nutzer-Schnittstelle) einer DApp hingegen muss nicht innerhalb der Blockchain verankert sein und kann in der externen Umgebung, wie bei üblichen Anwendungen ablaufen. Mit Blick auf die Anwendung von DApps werden unterschiedliche Felder ersichtlich, die im Folgenden in Kürze vorgestellt werden (Tuesta et al. 2015; DeRose 2016):

- 1) Token-Systeme zur Erstellung virtueller Zwillinge eines physischen Wertes: einen solchen Token kann man mit einer fälschungssicheren Wertmarke für einen eindeutig definierten Wertgegenstand in der realen Welt bezeichnen. Tokens dienen dem Nachweis von Eigentum in jeglicher Form (Währungen, Edelmetalle, Firmenanteile usw.) Des Weiteren können sie als Anreiz-Punktsystem genutzt werden.
- 2) Zahlungsverkehr und Derivate: DApps erlauben außerdem die dezentrale Speicherung von Derivaten in einer Blockchain oder Varianten des mobilen Bezahls. Aber auch der automatisierte, internationale Handel auf Finanzmärkten ist abbildbar.
- 3) Governance: Mit DApps werden die Kerneigenschaften von BCT (Manipulationssicherheit und Transparenz bei Anonymität) auch für die öffentliche Verwaltung greifbar. Vorstellbar sind hier Anwendungen wie der digitale Personalausweis oder Grundbucheinträge.
- 4) Datenspeicherung und -verwaltung: Mit dezentralen Cloud-Lösungen wird Speicherplatz angeboten und dabei dem Problem des „single point of failures“ erfolgreich begegnet. Dazu erfolgt eine Datenzerlegung und -verschlüsselung und deren Verteilung im Netzwerk.
- 5) IoT- und M2M-Kommunikation: hierbei ermöglichen die Funktionsweisen von Smart Contracts die Integration technischer Elemente in die Blockchain. Dabei kann über eine Blockchain-Plattform der Datenhandel autonom umgesetzt werden oder die Verwaltung von Daten abgebildet werden.

1.3 Technische Bewertung

Damit die Funktionsweisen einer verteilten Datenbankstruktur gewährleistet sind, gilt es drei relevante Charaktereigenschaften (kurz CAP) einzuhalten:

- 1) **Consistency** (eines gemeinsamen Zustandes) besteht dann, wenn alle Knotenpunkte des distribuierten Systems jederzeit den identischen Datenzustand einsehen können.
- 2) **Availability** ist erreicht, wenn das System im Rahmen einer tolerierbaren Antwortzeit sämtliche Anfragen von Knotenpunkten bearbeiten kann.
- 3) **Partition tolerance** umfasst ein fehlertolerantes Protokoll, sodass beim Ausfall eines Knotenpunktes oder bei Betrugs- bzw. Manipulationsangriffen von Knoten dennoch ein korrektes Ergebnis gesichert ist.

Das allgemeingültige CAP-Theorem nimmt jedoch an, dass immer nur zwei dieser beschriebenen Charakteristika zur gleichen Zeit in einem verteilten Datenbanknetzwerk erfüllt sein können (Angelis et al. 2017; Hammerschmidt 2017). Die noch recht junge Technologie hat vor diesem Hintergrund noch mit verschiedensten Herausforderungen und Limitationen zu kämpfen, für die aber derzeit unterschiedliche Lösungsansätze gesucht werden.

1.3.1 Technische Grenzen und Herausforderungen von Blockchain

Als bisher wohl anspruchsvollste Herausforderung von BCT wird in verschiedenen Quellen die Skalierbarkeit der Technologie beschrieben. So sind die Größen eines einzelnen Blocks begrenzt und damit eine Limitation der Transaktionsdurchsätze je Zeiteinheit gegeben. Die wohl naheliegende Lösung einer gesteigerten Blockgröße ist aus unterschiedlichen technischen Gründen praktisch nicht abbildbar.

So würden größere Blöcke zwar zu höheren Transaktionsraten führen, gleichzeitig aber auch einen erhöhten Rechenaufwand im Konsensprozess und damit verbundene erhöhte Energiebedarfe beanspruchen. V. a. die erhöhte Rechenleistung könnte zu einer vermehrten Zentralisierung der Ressourcen und einer steigenden Hardwareanforderung führen. Damit würden „kleinere“ Netzwerkteilnehmer systematisch aus dem Konsensprozess ausgeschlossen werden, was der Grundidee von verteilten Systemen widerspricht. Darüber hinaus führt eine Erhöhung der Blockgröße zu einer proportional steigenden Datenmenge, die gespeichert und übertragen werden muss, da nach der Speicherlogik Informationen zu sämtlichen vorangegangenen Transaktionen an den Knotenpunkten vorliegen. Teilnehmer bzw. Knotenpunkte mit einer geringeren Bandbreite wären auf dieser Grundlage schnell abgehängt. Damit liegt ein praktisches Problem größerer Blöcke nicht nur in der Bandbreite der Netzwerkteilnehmer, sondern auch in deren jeweiligen Speicherkapazitäten.

Neben dieser Kernherausforderung der Skalierbarkeit von Blockchain kommen weitere technologische Probleme hinzu, die im Folgenden aufgelistet sind:

- Gerade in Public Blockchains liegt eine essentielle Abhängigkeit in den Zugangsdaten (Public / Private Key). Verliert ein Nutzer seinen Schlüssel oder werden die Zugriffsdaten doch einmal gehackt, liegt bisher kein Ansatz zur Wiederherstellung vor.
- „Die Blockchain ist unveränderbar“. Dieser zitierte Vorteil der Technologie kann zugleich ein Nachteil sein. Wurde eine Transaktion fehlerhaft in das System gegeben, ist sie nachträglich nicht zu korrigieren.
- Ein wesentlicher Vorteil der Blockchain-Technologie liegt in der kryptographischen Verschlüsselung von Daten, deren Auflösung oder Manipulation wirtschaftlich irrationale Aufwendungen mit sich ziehen würde. Mit Blick auf die Entwicklungen im Bereich der Quanten-Computertechnik können sich die heute genutzten Sicherheitsansätze jedoch in der Zukunft als leicht überwindbar darstellen. So hat Google im September 2019 im Bereich der Quantencomputertechnik mit ‚Sycamore‘ erfolgreich eine Testaufgabe in 200 Sek. Gelöst, für die bisherige Supercomputer mathematisch ca. 10.000 Jahre benötigen würden (Drösser 2019)
- Bei den Konsensverfahren in Kap. 1.2.6 wurde bereits die Gefahr der Manipulation bei steigendem Machtanteil eines Netzwerkknotens beschrieben. Dieses Problem gilt es ebenfalls zu berücksichtigen.
- Darüber hinaus ist ein relevanter Anteil der heute möglichen Konsens-Verfahren nur unter der Anwendung einer Kryptowährung abbildbar, wie bspw. beim Proof-of-Stake-Verfahren.
- Öffentliche Blockchain-Lösungen gewährleisten Anonymität der Teilnehmer auf Basis von Pseudonymisierungs-Ansätzen. Transaktionshistorien können aber dennoch theoretisch nachvollzogen und mithilfe von Big Data-Anwendungen können möglicherweise bestimmte Gewohnheiten einzelner Nutzer abgeleitet werden. Sollte an der Schnittstelle zur realen Welt einmal der Nutzer hinter einem Pseudonym bekannt werden, können alle vergangenen Aktivitäten im Netzwerk nachvollzogen werden und auf diese Person zurückgeführt werden.
- Mit Blick auf Smart-Contract-Applikationen ist zu berücksichtigen, dass die Programmcodes eines Smart Contracts „open source“ sind und damit öffentlich lesbar. Beinhaltet ein solcher Code nun einen Fehler, der in der Konzeptionierung und Implementierung nicht erkannt wurde, kann er theoretisch von sämtlichen Netzwerkteilnehmern nachträglich ermittelt und zu den eigenen Vorteilen genutzt werden.
- Die Open-Source-Logik in der Blockchain-Technologie führt außerdem dazu, dass innovative Problemlösungen für die Technologie oftmals in unterschiedlichen Protokollen erfolgen und daraus eine zersplitterte Weiterentwicklung in Parallelstrukturen resultiert. Die Kompatibilität unterschiedlicher Blockchains bleibt

dabei auf der Strecke und es mangelt an einem einheitlichen Standard. Diesem Nachteil steht natürlich der Nutzen gegenüber, dass auf der Open-Source-Basis ganz individuelle, lösungsangepasste Blockchain-Konzepte entstehen können.

- Für eine branchenweite Adaption von Blockchain-Lösungen bedarf es neben einer technischen Standardisierung zudem einer notwendigen digitalen Infrastruktur.
- Ein zusätzlicher technischer Nachteil liegt sogleich im wesentlichen Vorteil der Blockchain-Technologie: So zeichnet sich die BCT als verteiltes Datenbanksystem durch die Sicherheit vor Manipulationen und Ausfällen aus, dabei ist diese Struktur aber immer ineffizienter und aufwendiger als ein zentrales System.
- **Sicherheit** – auch wenn die BCT als extrem sichere Technologie der Informationswissenschaften gilt, macht die folgende Übersicht deutlich, dass es in der IT nie eine absolute Sicherheit gibt. Im Bitcoin-Netzwerk wurde auf die bekannten Lücken bis jetzt jeweils eine Sicherheitslösung gefunden. Dennoch sind die bekanntesten Sicherheitsprobleme der Blockchain-Welt nachstehend aufgeführt (Meinel et al. 2018):

Denial-of-Service-Angriff	Gezielte Überlastung eines Netzwerkknotens, indem übermäßig viele Nachrichten an dieses Opfer versendet werden. Dieser Knotenpunkt wendet seine Ressourcen für die Bearbeitung der Nachrichten auf und steht dem Netzwerk nicht mehr zur Verfügung. Im Bitcoin-Netzwerk dienen gegen diese Art des Angriffs Reputationsregeln (Versand von falschen od. manipulierten Nachrichten werden mit Starfpunkten geahndet, bei 100 Punkten, wird entsprechende IP-Adresse für 24h gesperrt)
Flood-Angriff	Spam-Transaktionen: Angreifer versucht einen kompletten Block mit Transaktionen an sich selbst zu füllen, ohne Transaktionsgebühren einsetzen zu müssen. So könnten die Transaktionen anderer TN zeitlich verzögert werden. Im Bitcoin-Netzwerk gilt die 5%-Regel für gebührenfreie Transaktionen je Block, d. h. ein Angreifer müsste für 95 % der an ihn selbst gerichteten Transaktionen Transaktionskosten aufwenden, um das System anzugreifen.
Sybil-Angriff	Versuch, die Kommunikation im Netzwerk zu manipulieren, indem ein Angreifer mit mehreren, gefälschten Identitäten (Servern bzw. Knoten) im Netzwerk agiert. Angreifer hat so grundsätzlich die Möglichkeit, nur ausgewählte Informationen (Blöcke, Transaktionen) an Teilnehmer weiterzuleiten und damit Nutzer abzukapseln. In der Bitcoin-Blockchain wird dies durch eine Regulierung der Verbindung zu anderen TN versucht zu unterbinden.
51 % - Angriff	Verfügt ein Miner über mehr als 50 % der Rechenkapazität des gesamten Netzwerkes, hat er die Möglichkeit die Blockchain im Validierungsprozess neuer Informationen zu manipulieren. Sowohl PoW als auch PoS-Algorithmen sind von solchen Angriffen in der Theorie gefährdet.

- **Qualität der Daten** – der Übergang von physischer Welt in die Blockchain wird oft als Umsetzungsproblem von Blockchain außerhalb der Anwendung für Kryptowährungen

genannt. Betrug oder menschliche Fehler sind an diesem Übergang nur bedingt auszuschließen und können damit die gesamte Vertrauenswürdigkeit einer Blockchain-Anwendung (sofern bekannt ist, dass „falsche“ Daten in Blockchain sind) gefährden. Für dieses Problem kann Blockchain allein jedoch keine Lösung bieten. Hier gilt es bspw. mithilfe von IoT-Anwendungen oder Sensortechnik, künstlicher Intelligenz oder Big Data-Lösungen entsprechende Sicherheitslücken zu schließen und fehlerhafte Daten vor Aufnahme in die Blockchain zu identifizieren.

1.3.2 Heutige Grenzen und Herausforderungen von Blockchain-Technologie

Neben den technischen Herausforderungen bzw. Grenzen der Blockchain-Technologie, lassen sich weitere Limitationen aufführen. Zur Strukturierung der relevantesten Herausforderungen ist die nachfolgende Darstellung in fünf Kategorien unterteilt und betrachtet politische, wirtschaftliche, soziale, ökologische sowie rechtliche Herausforderungen – ergänzend zu den bereits erläuterten technischen Limitationen / Problemen von Blockchain.

Politische Herausforderungen:

- Grundsätzlich funktioniert eine Blockchain-Lösung staatenübergreifend und kann Akteure verschiedener Nationen ohne Intermediär oder staatliche Kontrollinstanz für Transaktionen oder den Austausch von Informationen und Werten zusammenbringen. Noch fehlt es an einer entsprechenden Gesetzgebung, die Haftungsfragen, die Gültigkeit von Smart Contracts oder Datenschutz einheitlich reguliert (Hosp 2018).

Wirtschaftliche Herausforderungen:

- Zahlungen können in Echtzeit ausgelöst werden. Ein **Zahlungsziel** auf Basis eines Smart Contracts zur erfüllten Gegenleistung kann heute noch nicht realisiert werden. Da technisch kein getrennter Ablauf von Eigentumsübergang und Auslösung einer Zahlung abbildbar ist. Dieses Problem wird sich aber voraussichtlich relativ schnell durch technische Weiterentwicklung lösen lassen (Drescher 2017).
- BCT steckt in den Kinderschuhen. Konkrete Kosten-Nutzen-Analysen über Investitions- und operative Kosten für den Betrieb einer BCT-Lösung sowie dem gegenüberstehende Effizienzgewinne werden erst in einzelnen Projekten validiert (Walport 2015).
- Mangelnde Standards für eine branchenweite oder gar branchenübergreifende Industrielösung führt bisher zu zahlreichen untereinander nicht-kompatiblen Blockchain-Anwendungen (Meinel et al. 2018).
- Soll die Systeminfrastruktur angepasst, geändert oder weiterentwickelt werden, muss die Mehrheit der Systemteilnehmer einer solchen technischen Anpassung vorab

zustimmen, da es sonst technisch, wie auch organisatorische mit Hilfe einer sog. Fork⁵ zu einer Absplitterung im Netzwerk kommt. Bis also evolutionäre Optimierungen der Technologie in einem Netzwerk umgesetzt sind, bedarf es eines aufwendigen Abstimmungsprozesses, der selten Erfolg für eine einstimmige Umsetzung garantieren kann (Meinel et al. 2018).

Soziale Herausforderungen:

- Wie für jede junge Technologie gilt auch für die BCT: Die Akzeptanz ggü. der Technologie muss bei Unternehmen und Gesellschaft erst wachsen und Ängste sowie Vorurteile ggü. dem „Unbekannten“ durch Aufklärung abgebaut werden.
- Paradigmenwechsel von Informationen als Wettbewerbsvorteil in Silos zur Optimierung und Entwicklung ganzer Branchenvorteile durch Transparenz. Hierhin liegt eine Herausforderung, die noch vor der eigentlichen Implementierung von Blockchain liegt (Palka und Wittpahl 2018).

Ökologische Herausforderungen:

- Ein Problem von Public Blockchains liegt im ressourcen-intensiven Konsensverfahren zur Validierung neuer Transaktionen (Proof-of-Work). Der Stromverbrauch hierfür ist immens und wird oftmals kritisiert. Bei privaten oder konsortialen BC werden jedoch deutlich energieeffizientere Konsensverfahren genutzt, die dieses Problem bereits erfolgreich lösen (Hosp 2018).

Rechtliche Herausforderungen:

- Datenschutz und Datensicherheit – ähnlich den Herausforderungen aus politischer Sicht, ist ungeklärt, wie mit Datenschutz und Datensicherheit in einer Blockchain – die nicht einer Instanz „gehört“ und für die niemand voll haftbar gemacht werden kann, umgegangen wird (Schlatt et al. 2016; Schütte et al. 2017).
- Nach EU-DSGVO Artikel 17 herrscht das Recht auf Löschung bzw. „Vergessen werden“. Diese rechtliche Anforderung ist in öffentlichen Blockchains bisher technisch nicht umsetzbar (Voshmgir 2016).
- Kartellrechtliche Fragestellungen entstehen bei konsortialen Blockchain-Anwendungen, bei denen sich die großen Akteure einer Branche zusammenschließen und daraus ggf. Wettbewerbsvorteile generieren (Hosp 2018).

⁵ Fork (dt. Gabelung) bezeichnet eine Abspaltung der bis dahin bestehenden Blockchain in einen modifizierten Quellcode. Heißt, die bestehende Blockchain wird weitergeführt und eine zusätzliche Version entsteht auf Basis des bereits genutzten Quellcodes, allerdings mit ergänzten Änderungen. Sind die Nutzer des bisherigen Systems nicht kompatibel zum neu entstanden System, erfolgt eine komplette Abspaltung bzw. Aufteilung der Nutzer auf das alte und neue System.

- Die juristische Bedeutung eines Smart Contracts ist ungeklärt, wer wann in einem solchen Kontext haftbar gemacht werden kann, und wie Verstöße außerhalb der Blockchain geahndet werden können bleibt offen. Noch gilt die Blockchain als eine Art „rechtsfreier“ Raum (Schütte et al. 2017).

An dieser Stelle ist festzuhalten, dass sich die erläuterten Herausforderungen einen aktuellen Status quo in Bezug auf den jetzigen Stand der Technik darstellen. Die rasante technische Weiterentwicklung kann erläuterte Herausforderungen innerhalb kürzester Zeit redundant machen und zugleich neue, bisher unbekannte Herausforderungen bzw. Limitationen mit sich bringen. Neben den erläuterten Herausforderungen werden im folgenden Abschnitt die Chancen bzw. Potentiale von BCT zusammengefasst.

1.3.3 Technische Chancen und Potenziale

Die Möglichkeiten, die sich durch Blockchain-Technologie auftun, lassen sich in bereits bestehende und perspektivische Potenziale aufteilen. Aus den vorangegangenen Absätzen sollte ersichtlich geworden sein, dass Blockchain einem hohen Maß an Sicherheitsansprüchen gerecht werden kann. Nach den bisherigen Entwicklungen liegt ein wesentlicher Vorteil in der **Datenintegrität** und **Manipulationssicherheit** der jeweils zugrundeliegenden Konsens-Mechanismen. Damit kann ein **vertrauensvolles Netzwerk** geschaffen werden, **ohne** dass es **Vertrauen zwischen den einzelnen Teilnehmern** bedarf. Ein weiterer Nutzen liegt in der hohen technischen **Zuverlässigkeit** des Netzwerks, da ein „**Single-Point-of-Failure**“ **ausbleibt**. Blockchain steht für **Transparenz**, die durch das verteilte, manipulationsgeschützte und ggf. öffentlich einsehbare Blockchain-System sichergestellt ist. Dabei liefern Smart Contracts heute schon einen beachtenswerten **Automatisierungsgrad** und erlauben dank der Möglichkeiten von Smart Contract Oracles die **Einbindung von externen Systemen und Zuständen**. An der anderen Seite – ggü. dem Nutzer – wird mit den sog. **DApps eine Schnittstelle** geschaffen, mit der die Technologie auch weniger technisch-versierten Nutzern zugänglich wird. Ebenfalls liefert der **Open Source-Gedanke** bereits heute die Potenziale von **vielfältigen, individuell**, auf die Bedürfnisse angepassten Abwandlungen der Blockchain-Lösung (Hosp 2018).

Mit Blick auf die im nachfolgenden Kapitel erläuterten Weiterentwicklungen innerhalb der Blockchain-Technologie und darüber hinaus lassen sich noch weitere Potenziale von Blockchain für die Zukunft ableiten (Bogensperger et al. 2018):

- So kann durch neue Formen des Konsens-Prozesses, die Anwendung **alternativer Distributed Ledger Technologien** (wie z. B. ‚Tangles‘ oder ‚Hashgraphs‘) oder sog. ‚State Channels‘ die **Transaktionsrate optimiert** werden.

- Bei einer **alternativen Programmierung von Smart Contracts** mithilfe von funktionalen Programmiersprachen lässt sich die **Sicherheit erhöhen**.
- **Normungen** und auch technologische Entwicklungen lassen derzeit auf eine perspektivisch **optimierte Interoperabilität unterschiedlicher Blockchain-Protokolle** hoffen.

1.3.4 Technische Weiterentwicklungen von Blockchain

Sicherheitslücken von Smart Contracts: Die Potenziale von Smart Contracts wurden bereits in Kapitel 1.4.7 näher erläutert und es wurde auf damit einhergehende Risiken bzw. Herausforderungen eingegangen. So ist deren Code meist für alle Teilnehmer frei zugänglich. Mit der Verzahnung von Smart Contracts mit oftmals finanziellen Entlohnungen besteht daher das große Interesse unter den Nutzern, Programmierungs-Schwachpunkte zu ermitteln, auszunutzen und sich an Millionenbeträgen aus dem Netzwerk zu bereichern. Eine Studie der National University Singapur hat im Jahr 2018 insgesamt über 970.000 Smart Contracts des Ethereum-Netzwerks auf entsprechende Fehler untersucht: 3,5 Prozent aller untersuchten Smart Contracts (ca. 34.000) enthielten Sicherheitsmängel, die einen Schaden von rund 2,9 Mio. US-Dollar hätten verursachen können (Ivica et al. 2018). Grund für diese Sicherheitsprobleme in Smart Contracts liegt u. a. in der aufwendigen Kontrolle und Fehleranalyse von imperativen Programmiersprachen. Dabei bedarf es Simulationen, Testrunden oder Peer Reviews und dennoch liegt die Gefahr vor, dass die Programmcodes nicht sorgfältig genug geprüft werden können. Dem gegenüber steht die funktionale Programmierung, bei der anhand von Mathematik ergründet werden kann, ob solche Sicherheitslücken bestehen (Manoury 2007). Ein Beispiel für eine solche Weiterentwicklung von Smart Contracts auf funktionaler Basis liefert die ‚Cardano‘-Blockchain, um Sicherheit von Smart Contracts quantifizierbar zu machen (Hoskinson 2018).

Normung: Die Internationale Organisation für Normung (ISO) hat bereits ein Komitee für Blockchain und Distributed Ledger Technologien (ISO/TC 307) ins Leben gerufen, um sich mit Normungen und der Kompatibilität verschiedener Blockchain-Ansätze zu befassen. Dabei wird v. a. auch das Thema der Kompatibilität als relevanter Erfolgsfaktor der Technologie angesehen, wenn verschiedene Blockchain-Systeme interoperabel agieren sollen (Bogensperger et al. 2018).

Skalierbarkeit: Der bislang wesentlichsten Herausforderung der Blockchain-Technologie stehen vielfältige Lösungsansätze gegenüber, um die Skalierbarkeit und damit auch die Transaktionsgeschwindigkeit in einem Blockchain-System zu optimieren. Über die drei bekanntesten Ansätze wird im Folgenden eine kurze Übersicht gegeben (Walport 2015):

- 1) **Sidechains:** Unter diesem Begriff werden im Grunde interoperable Blockchains zusammengefasst, zwischen denen Transaktionswerte getauscht werden können. D. h., Werte bzw. Objekte der „Hauptkette“ können auf eine entsprechende Sidechain überschrieben werden und wieder in die Hauptkette zurückgeführt werden. Damit können Funktionalitäten der Blockchain selbst problemlos ausgelagert werden und Skalierungsprobleme teilweise gelöst werden. Gleichzeitig führen Sidechains zu einer gesteigerten Komplexität.
- 2) **State Channels:** Ein weiterer Ansatz um Skalierbarkeit zu optimieren, liegt in sog. State Channels. Dabei werden Mikrotransaktionen außerhalb der Blockchain ausgeführt und gebündelt. So wird nicht mehr jede einzelne Transaktion in der Blockchain selbst gespeichert, sondern nur ein validierter Endzustand in die Hauptkette gegeben. So lassen sich mehr Transaktionen je Sekunde realisieren. Dabei steigt aber auch die Intransparenz in der Nachvollziehbarkeit von durchgeführten Transaktionen.
- 3) **Sharding:** dieser Ansatz wird bisher in der Fachliteratur nur theoretisch diskutiert und noch nicht implementiert. Die Idee liegt aber in der Aufteilung von Transaktionsdaten innerhalb eines Blockchain-Netzwerks. So werden im Gegensatz zu den üblichen Blockchain-Lösungen nicht mehr die Transaktionsdaten aller Netzwerkteilnehmer validiert und gespeichert, sondern nur noch von einem kleineren Anteil der Nodes. Auf diese Weise findet eine distribuierte Validierung, kombiniert mit einer verteilten Speicherung der Daten innerhalb der Blockchain statt. Die Umsetzung kann dann in sog. Shards erfolgen, in denen jeweils nur ein Teil des Status quo mit den dazugehörigen Transaktionen und den dabei involvierten Knotenpunkten gesichert ist (Zamani et al. 2018).

2 Entwicklungen von BCT im Agri-Food-Sektor und Anwendungsfelder

Die Anwendung von Blockchain-Technologie in der Agrar- und Lebensmittelbranche ist bereits in Form von Pilotprojekten, Business Cases von Start-ups und ersten Roll-Outs zu beobachten. Das nachfolgende Kapitel gibt einen Marktüberblick hinsichtlich der Fragestellung, welche Akteure sich mit der Blockchain-Technologie bereits auseinandersetzen, wo und durch welche Player Konsortien entstanden sind und in welchen Regionen die Anwendung von Blockchain-Technologie besonders ausgeprägt ist. Zudem lässt sich eine Clusterung der untersuchten Use Cases vornehmen. Auf diese Weise kann für die weitere Marktbeobachtung eine entsprechende Fokussierung vorgenommen werden.

2.1 Marktübersicht von Blockchain-Projekten im Agri-Food-Sektor

Im Rahmen der Marktanalyse wurden über 85 Use Cases untersucht, in denen zwischen 2016 und 2019 die Anwendung von Blockchain-Technologie im Agrar- und/oder Lebensmittel-Sektor erprobt bzw. bereits etabliert wurde. Methodisch wurden dabei Use Cases in der Analyse berücksichtigt, die bereits in wissenschaftlichen Artikeln behandelt wurden sowie Pressemitteilungen und Online-Berichte von verschiedenen IT- und Branchen-News-Webseiten, die sich auf Blockchain-Technologie spezialisiert haben. Weitere Use Cases wurden über die Datenbank Google mit folgendem Suchstring „(Blockchain OR Distributed Ledger) AND (Agri* OR Food*)“ ermittelt. Im Anhang findet sich eine Auflistung aller berücksichtigten Use Cases, mit Angaben zu involvierten Akteuren, einer kurzen Beschreibung des Anwendungsbeispiels sowie Region und Projektstart. Ebenso sind dort die Quellenangaben zu allen in Kapitel 2.1 genannten Anwendungen aufgeführt.

Bei der Kategorisierung der analysierten Use Cases nach den involvierten Playern wurde eine Unterteilung nach den einzelnen Stufen innerhalb der Wertschöpfungskette vorgenommen. Vorgelagerte Stufen von Agri-Food-Chains, wie Agro-Chemie, Saatgut-Produktion oder Agrartechnik sind dabei zusammengefasst. „Commodity“ umfasst zudem Finanzinstitute, die im internationalen Rohstoffhandel involviert sind. Des Weiteren finden eine Unterteilung der Unternehmen nach den Bereichen „Landwirtschaft und Erzeugung“, „Lebensmittel-Verarbeitung“, „Logistik“ und „Handel“ statt. Neben Playern der Lieferkette selber wurden zudem Projekte von staatlichen Instanzen, Non-Profit-Organisationen und Zertifizierungsgesellschaften sowie Konsortien unterschiedlicher Akteure berücksichtigt. Bisher unbekannte Player, die in Form von Start-Ups auf den Markt treten und sich durch Blockchain-Lösungen im Agri-Food-Bereich auszeichnen, sind ebenfalls berücksichtigt. Die folgende Abbildung zeigt involvierte Player nach der Kategorisierungslogik auf.

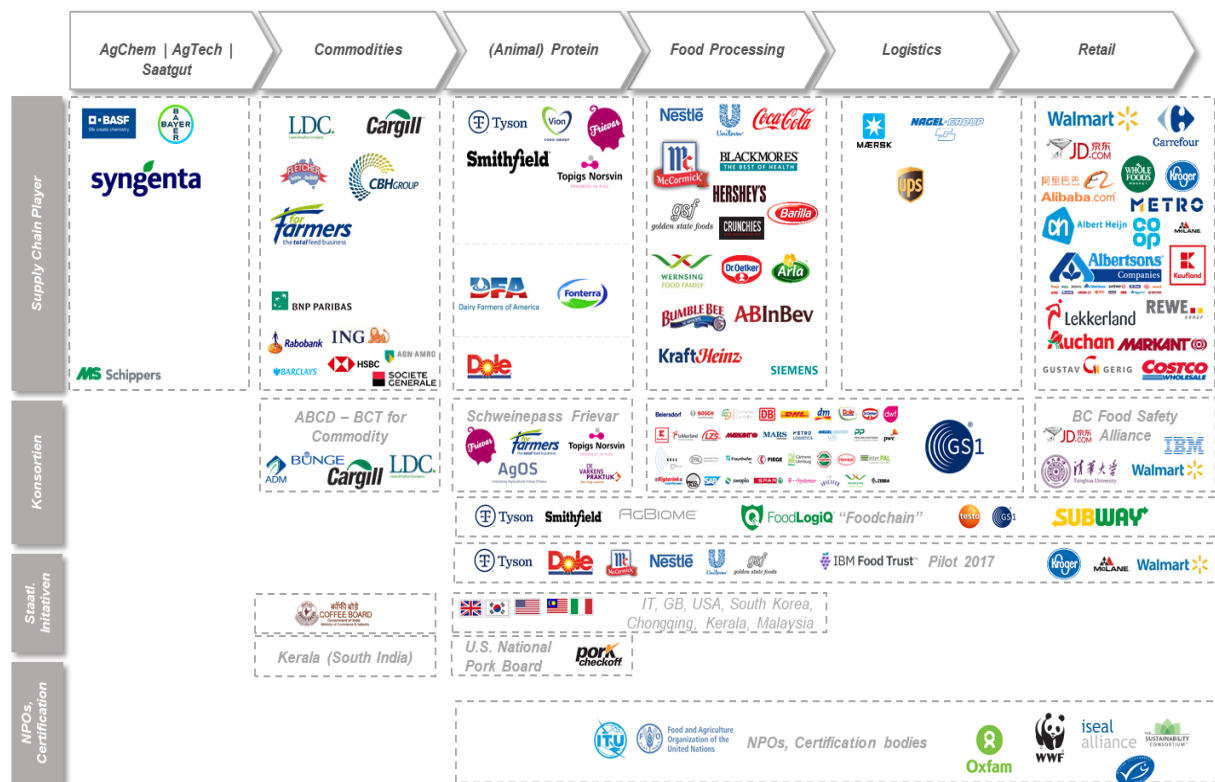


Abb. 8: Agri-Food-Akteure mit Blockchain-Pilotprojekten (eigene Darstellung)

Über alle Cluster hinweg ist dabei eine Fokussierung auf das Thema Rückverfolgbarkeit von Lieferketten sowie der Steigerung von Lebensmittelsicherheit zu sehen. Bei 46 analysierten Anwendungsbeispielen liegt die **Motivation** explizit in der **Optimierung von Rückverfolgbarkeit und Lebensmittelsicherheit in Lieferketten** sowie der **Steigerung des Verbrauchervertrauens mittels erhöhter Transparenz**. Vor allem die staatlich-initiierten Projekte sowie Anwendungsbeispiele durch Akteure des LEHs zielen auf dieses Anwendungsfeld von Blockchain-Technologie ab.

Teilweise wird in diesen Anwendungsfeldern die Optimierung von Nachhaltigkeitsperformance bzw. der glaubwürdige und transparente Nachweis über die Einhaltung spezieller Nachhaltigkeitsanforderungen entlang einer Lieferkette ergänzend oder sogar schwerpunktmäßig fokussiert. Dieser Fokus ist v. a. bei entwickelten Lösungen von Start-ups zu beobachten, die mitunter neben der Agrar- und Foodbranche eine Vermarktung ihres Leistungsangebotes bspw. für die Textilindustrie oder Luxusgütern, wie Diamanten anbieten.

Bei Betrachtung der einzelnen Projekte wird deutlich, dass der überwiegende Anteil an Projekten bisher von Akteuren des Lebensmitteleinzelhandels getrieben wurde. Walmart startete zusammen mit IBM im Jahr 2016 die ersten Pilotversuche und involvierte weitere Akteure der vorgelagerten Stufen. In Europa gehört Carrefour zu den Treibern von Blockchain-Projekten im LEH. Weitere Treiber sind von der „anderen Seite der Kette“ zu identifizieren. So gehören die globalen Player des Rohstoffhandels (Cargill, Louis Dreyfus und CBH) zu den

ersten Akteuren, die sich mit der Anwendungsmöglichkeit von BCT für den internationalen Rohstoffhandel in Kooperation mit entsprechenden Finanzinstituten auseinandergesetzt haben. Cargill verfolgte indes aber ein weiteres Projekt zur Rückverfolgbarkeit von Truthähnen zu Thanksgiving in den USA und bildete dazu eine vollintegrierte Produktionskette vom Futtermittel bis zum Supermarkt auf BC-Basis ab.

Weiterhin ist die Aktivität staatlicher Projekte zu berücksichtigen. So sind seit 2018 diverse staatlich initiierte Projekte in Kooperation mit Landwirtschafts- und Ernährungsministerien zur Erhöhung der Rückverfolgbarkeit und daraus resultierender optimierter Lebensmittelsicherheit und Transparenz für den Verbraucher zu beobachten. Gegenstand der Pilotprojekte ist dabei immer wieder die Lieferkette bzw. Lieferkettenabschnitte von Rindfleisch. Neben Projekten im asiatischen Raum beschäftigt sich die Food Safety Agency (FSA) in Großbritannien oder die U.S. Food and Drugs Administration mit BCT zur Rückverfolgbarkeit von Lebensmitteln. Das italienische Ministerium für Agrarwirtschaft und Lebensmittelsicherheit kooperiert seit Mai 2019 mit Kraft Heinz, um die Lebensmittelsicherheit in Babynahrung mithilfe von BCT zu erhöhen.

Neben Playern der Wertschöpfungskette und staatlich initiierten Projekten haben sich zudem diverse Start-ups mit dem Fokus auf BCT im Agrar- und/oder Lebensmittelsektor aufgetan. Eine verstärkte Gründungsphase in diesem Feld ist in den Jahren 2016 und 2017 zu beobachten. Auch unter den Start-ups liegt das wesentliche Anwendungsgebiet von BCT in der Rückverfolgbarkeit und erhöhten Transparenz von Lebensmittellieferketten. Daneben zeichnen sich Geschäftsmodelle ab, mit denen ein direkter Handel zwischen Kunde und Lieferant auf einer Online-Plattform ohne einen Mittelsmann möglich ist. Start-ups, die auf dieses Anwendungsgebiet ihren Fokus legen, richten sich i. d. R. an kleine Akteure in Value Chain Systemen, denen bisher ein lukrativer Marktzutritt verwehrt bleibt. Ähnlich zu diesem Anwendungsfeld finden sich zudem Start-ups, die sich mit BCT-Anwendungen aus anderen Branchen an die Herausforderungen von Kleinbauern in Entwicklungs- und Schwellenländern richten. Dazu zählen beispielsweise automatisierte Ernteausfallversicherungen, Micro-Kredite oder Shared-Economy-Mietmodelle für Traktoren und Landmaschinen.

Neben Start-ups mit dem Fokus auf Blockchain-Lösungen im Agri-Food-Sektor sind weitere Stakeholder im Blockchain-Ecosystem für die Branche zu berücksichtigen. Einzelne Unternehmensberatungen mit IT-Schwerpunkt haben sich bspw. auf die Anwendung von BCT im Supply Chain Management oder speziell auf den Agrar-/Lebensmittelbereich fokussiert. Weiterhin spielen in diesem Kontext IT-Serviceanbieter eine Rolle. Neben IBM – als Vorreiter auf dem Blockchain-Feld für Lebensmittellieferketten – sind SAP, Intel, Amazon Web Services oder Microsoft Azure in Pilotprojekten involviert. Siemens arbeitet derweil an einer BC-basierten Lösung zur Rückverfolgbarkeit von Kartoffelchips ohne einen Partner aus der Lieferkette dabei zu nennen.

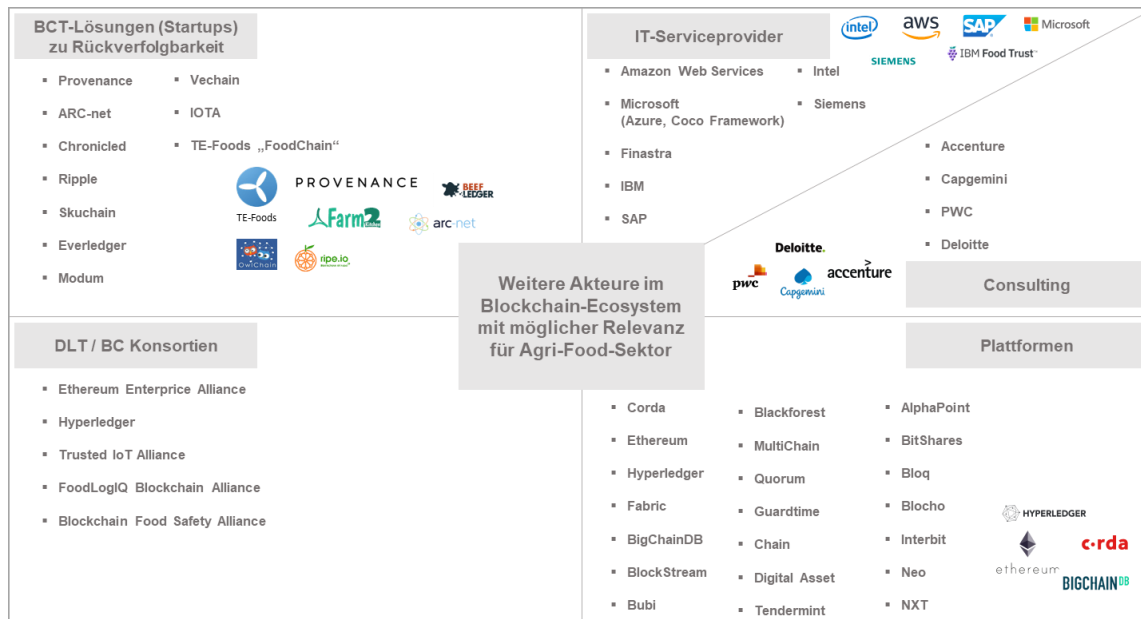


Abb. 9: Bereits relevante Akteure für den Ag/Food-Bereich im Blockchain-Ecosystem

Bei der Betrachtung des Ökosystems von BCT gilt zudem die Abgrenzung von Blockchain- bzw. DLT-Konsortien, von denen oftmals eine entsprechende Plattform zur Nutzung der Technologie ausgeht. In Projekten des Agri-Food-Sektors werden Lösungen vermehrt auf Basis der Ethereum-Blockchain oder Hyperledger (u.a. IBM FoodTrust) erarbeitet.

Weiterhin zu beobachten sind aber auch Konsortien, die sich speziell für die Entwicklung von BCT-Anwendungen auf Lebensmittelherausforderungen zusammengeschlossen haben. Neben der *Blockchain Food Safety Alliance*, die sich aus Walmart, IBM, JD.com und der Tsinghua University National Engineering Laboratory for E-Commerce Technologies bereits 2016 formiert hat, ist das konsortiale Projekt von FoodLogIQ von Relevanz. FoodLogIQ bietet bereits seit 2006 Rückverfolgbarkeit von Lebensmittellieferketten als SaaS an. Zusammen mit Tyson Foods, Smithfield, Testo, Subway und weiteren Partnern arbeitet das kanadische IT-Startup für Monitoring und Rückverfolgbarkeit im Lebensmittelbereich seit Q3 2018 an BCT-Pilotprojekten. 2017 zählte FoodLogIQ dabei nach Forbes zu den 25 innovativsten Startups im AgTech-Bereich (FOODLOGIQ 2019). In Deutschland ist bisher erst ein konsortiales Blockchain-Projekt mit Playern der Branche durchgeführt worden bzw. bekannt. GS1 Germany initiierte mit über 30 Partnern aus Logistik, IT, Handel und Produktion ein Projekt zum digitalen Tausch von Europaletten auf Blockchain-Basis. Aus dem Lebensmittelsektor waren dabei Dr. August Oetker Nahrungsmittel KG, Dole, Wernsing Food Family, Markant, Mars, SPAR, Lekkerland, Kaufland sowie Vöslauer beteiligt. GS1 als Standardgeber für eine einheitliche Produktidentifikation und -kommunikation in Lieferketten sämtlicher Branchen, verfolgt dabei das Ziel, Supply Chain Management effizienter und unternehmensübergreifend nachvollziehbarer zu gestalten. Mit dem Projekt zum digitalen Palettschein auf einer

Blockchain-Anwendung hat sich GS1 erstmalig mit den Anwendungspotenzialen der neuen Technologie in der Praxis auseinandergesetzt.

Als Katalysator für konsortiale Blockchain-Projekte im Agri/Food-Bereich kann wohl der Zusammenschluss von IBM und Walmart in 2016/17 gesehen werden. In einem ersten Pilotprojekt wurde die Rückverfolgbarkeit von Lebensmitteln auf der von IBM entwickelten Lösung „IBM Food Trust“ mit Akteuren, wie Nestlé, Unilever, Tyson Foods oder Dole erprobt. Im Oktober 2018 fand der Launch der IBM Plattform auf Hyperledger-Basis statt. Seitdem versprechen sich gerade auf dem europäischen Markt Akteure des Lebensmitteleinzelhandels Nutzen von „IBM Food Trust“. Carrefour hat seit Mitte 2018 bereits mehrere Projekte in Kooperation mit IBM gestartet und vertreibt die ersten Produktlinien mit „Blockchain-Rückverfolgbarkeitslösung“ in Spanien, Frankreich und Italien. Seit März 2019 kooperiert Carrefour zudem mit Nestlé zur Rückverfolgbarkeit von verarbeiteten Produkten. Hierbei startete ein erster Versuch mit Instant-Kartoffelpüree.

Mit Blick auf die zeitliche Entwicklung von Blockchain-Anwendungen in der Branche wird deutlich, dass erst mit der technischen Entwicklung der sog. 2. Blockchain-Generation, sprich Ethereum usw., die Anwendung in Lieferketten und damit auch im Agri-Food-Bereich denkbar wurde. Erste Projekte wurden im Herbst 2016 angekündigt und in Pilot-Phasen konzipiert und getestet. Nachdem im Folgejahr schließlich die ersten „Erfolgsmeldungen“ von namenhaften Akteuren gemeldet wurden und die technische Weiterentwicklung bereits einen Teil der anfänglichen Probleme beheben konnte, ist im Jahr 2018 ein Hype unter den Branchenplayern zu beobachten. Waren es 2017 noch 13 bekanntgegebene Projekte, wurden in der Analyse für das Jahr 2018 insgesamt 39 Projekte erfasst. Dabei wurden einmalige Pressemeldungen von angekündigten Projekten, ohne Folgemeldungen bzw. Ergebnisbericht oder inhaltlich-/technisch-weiterführende Erläuterungen vom Projektträger selbst, in der Analyse nicht weiterberücksichtigt. Wenngleich sich solche Meldungen aus dem Jahr 2018 ebenfalls in einer Vielzahl finden lassen. Ähnlich der generellen Entwicklung von Blockchain-Technologie nach dem Gartner Hype Cycle for Emerging Technologies, ist auch eine Abnahme des Hypes um die Technologie in der Agri-/Food-Branche im Jahr 2019 zu beobachten. Bis Juni 2019 wurden insgesamt 15 Projekte in der Analyse berücksichtigt. Zu beachten ist aber, dass einzelne Pilotprojekte, die in 2018 initiiert wurden, nach erfolgreicher Testphase ein Roll-Out für 2019 oder 2020 angekündigt haben. Dazu zählen bspw. Carrefour, Albert Heijn, Walmart und Cargill.

Die nachfolgende Abbildung stellt die analysierten Projekte geclustert und nach ihren jeweiligen Startterminen zwischen den Jahren 2016 und 2019 dar.

	2016 / 2017	2018	2019
Start-up Gründungen	<ol style="list-style-type: none"> 1. AgriLedger 2. Provenance 3. Demeter.Life 4. Ripe 5. Ambrosus 6. OriginTrail 7. ARC-net 	<ol style="list-style-type: none"> 8. BEXT360 9. HARA 10. Hello Tractors (IBM) 11. TwingaFoods (IBM) 12. BeefLedger 	
Staatl. Projekte		<ol style="list-style-type: none"> 1. Südkorea 2. Food Safety Agency (GB) 3. USFDA 4. Kerala State (Indien) 	<ol style="list-style-type: none"> 5. FAO, ITU 6. Provinz Chingping China 7. Malaysia
Konsortien, Allianzen	<ol style="list-style-type: none"> 1. Walmart Food Safety Alliance (China) 2. IBM Food Trust Pilot 	<ol style="list-style-type: none"> 3. Dairy Farmers of America (DFA) 4. GS1-Pilot 5. ABCD-Konsortium 6. FoodLogIQ (Konsortium) 7. BeefChain (Australien) 	<ol style="list-style-type: none"> 8. US National Pork Board 9. Coffee Board of India
Projekte mit / von Playern der Branche	<ol style="list-style-type: none"> 1. CBH + AgriDigital 2. Crunchies 3. Nestlé (Start m. BC-Projekten, mittlerweile über 10 Projekte) 4. Cargill + Intel 	<ol style="list-style-type: none"> 5. Alibaba, Fonterra, Blackmores, PWC 6. Alibaba, JD.com 7. BASF m. ARC.net 8. Bayer Crop, BlockApps, ConsenSys 9. Louis Dreyfus 10. Arla Milkchain 11. Barilla + IBM 12. Tyson Foods 13. Maersk 14. WWF 15. Oxfam 16. Carrefour 17. Gustav Gerig 18. The Co-Op 19. REWE 20. Anheuser 21. AUCHAN 22. Coca-Cola 23. Frievar, AgOS, MS Schippers, For Farmers – Schweine-Pass 24. Albert Heijn 	<ol style="list-style-type: none"> 25. Golden States Food 26. Hershey Chocolate Company 27. Siemens Kartoffelchips 28. WWF mit eigener Blockchain 29. Metro + Deepshore 30. Albertsons 31. Carrefour, Nestlé, IBM 32. BumbleBee Foods + SAP 33. Carrefour Produktlinie auf BC-Basis

Abb. 10: Agri-Food-Blockchainprojekte von 2016 bis 2019 (i.A. an Anhang 1)

Eine jeweils zusammenfassende Beschreibung der berücksichtigten Blockchain-Projekte im Rahmen der Analyse ist der beigefügten Excel-Übersicht „Marktanalyse“ zu entnehmen. Quellenangaben zu den einzelnen Projekten / Use Cases sind ebenfalls dem Anhang 1 in Spalte I zu entnehmen.

2.2 Clusterung bisheriger Anwendungsfälle mit Relevanz für Lebensmittellieferketten

Der nachfolgende Abschnitt basiert auf den untersuchten Anwendungsbeispielen und wissenschaftlichen Publikationen zur Anwendung von BCT im Agrar- und Lebensmittelbereich bzw. dem Supply Chain Management (SCM). Dabei wird die Anwendung von Blockchain in die für Lebensmittellieferketten relevanten Bereiche ‚**Supply Chain Management**‘, ‚**Auditierung bzw. Zertifizierung**‘ sowie ‚**Internet of Things-Anwendungen (IoT)**‘ unterteilt. Für das erste Feld „SCM + Logistik“ wird aufgrund der umfangreichen Anwendungsmöglichkeiten eine weitere Unterteilung in drei Unterkategorien: Internationaler Warenaustausch, Rückverfolgbarkeit und Echtzeitlokalisierung gegeben. Für jedes der erläuterten Anwendungsfelder werden jeweils heutige Herausforderungen in Kürze erläutert. Darauf aufbauend erfolgt eine Darstellung der Lösungspotenziale von Blockchain sowie eine Beschreibung eines oder mehrerer Anwendungsbeispiele. Eine stichpunktartige Darstellung bestehender Grenzen bzw. Herausforderungen von Blockchain-Anwendungen im jeweiligen Cluster schließt die folgenden Teilkapitel ab.

2.2.1 Supply Chain Management

Diverse Studien haben in den letzten Jahren das Potenzial der Blockchain-Technologie in unterschiedlichen Branchen und Anwendungsbereichen untersucht. Neben der Finanzwirtschaft werden in den verschiedensten Publikationen die Logistikbranche und das Supply Chain Management als Kernanwendungsfelder der disruptiven Technologie genannt (z. B. Schlatt et al. 2016; Brandt et al. 2018). Mit Blick auf die Möglichkeit, Transparenz in Lieferketten zu erhöhen, wird in einer Studie des Weltwirtschaftsforums großes Potenzial in der Verbesserung von Lieferbeziehungen einzelner Supply Chain Akteure gesehen (Herwijer et al. 2018). Speziell für die Automobilindustrie, aber dennoch übertragbar auf Supply Chains anderer Branchen, sind die Ergebnisse einer Studie herausgegeben von Roland Berger im Jahr 2018. Demnach werden wesentliche Anwendungspotenziale von Blockchain in der Rückverfolgbarkeit von einzelnen Bauteilen sowie der Echtheitszertifizierung und -identifizierung von Fahrzeuersatzteilen gesehen (Boyle et al. 2018). Auch unter Supply Chain Managern und Führungskräften sehen laut einer Befragung der Hermes Germany GmbH (2018) rund ein Drittel der insgesamt Befragten in der Blockchain-Technologie „ein Veränderungspotenzial [...], dass über das Potenzial des normalen Digitalisierungsprozesses hinausgeht“ (Hinckeldeyn 2019). Dabei wird allen voran ein wesentlicher Mehrwert von Blockchain für das Supply Chain Management in der Verschlinkung administrativer Prozessanforderungen, der sicheren Nutzung von IoT-Lösungen und dem Schutz vor Produktfälschungen sowie in Herkunftsnachweisen gesehen (Hackius und Petersen 2017).

2.2.1.1 Aktuelle Problemstellungen

Als wesentliche Herausforderungen im Supply Chain Management wird in der Literatur und in diversen Studien die zunehmende Komplexität von Lieferketten, v.a. mit Blick auf den Individualisierungstrend der Verbraucher und die steigende Internationalisierung von Wertschöpfungsketten gesehen. Damit einher geht zudem die Gefahr von Produkt- und Dokumentenfälschung, wodurch mitunter die Reputation eines Zulieferunternehmens im internationalen Handel gefährdet sein kann. Um diesen Herausforderungen vorzubeugen werden aufwendige administrative Prozesse im SCM an jeder einzelnen Schnittstelle einer kompletten Lieferkette realisiert. Teilweise führen die heute noch papierlastigen Prozesse damit zu Verzögerungen der Lieferungen (Leong et al. 2018). Verschiedenste IoT-Lösungen wurden für diese Herausforderungen bereits entwickelt, versprechen aber bisher noch nicht die endgültige Manipulationssicherheit bereits gespeicherter Daten sowie an der Schnittstelle zwischen physischer Welt und Sensoren (Sallaba et al. 2018). Geht es darum, die Rückverfolgbarkeit von fehlerhaften Produkten zu garantieren, nutzen Hersteller und Vermarkter i. d. R. zentrale Systemlösungen spezieller Track+Trace Anbieter. Die Abhängigkeit von solchen Dienstleistern spiegelt sich dabei nicht nur kostentechnisch, sondern auch in der Funktionsfähigkeit der Systeme wider. Eine lückenlose und exakte Rückverfolgbarkeit über alle Stufen einer Wertschöpfungskette hinweg, stellt dabei mit der steigenden Komplexität von Produkten und Lieferstrukturen eine der Kernherausforderungen im Supply Chain Management dar (Casado-Vara et al. 2018).

2.2.1.2 Lösungspotenziale und Anwendungsbeispiele

Wie bereits zu Beginn des Kapitels angeführt, fokussieren bisherige Pilotprojekte und theoretische Überlegungen zu den Anwendungsmöglichkeiten von Blockchain im Supply Chain Management v.a. die Verschlinkung administrativer Dokumentationsprozesse sowie die Transparenz in Lieferketten und zwischen den unterschiedlichen Akteuren. Untersuchte Projekte und Studien zeigen, dass sich dabei die Lösungspotenziale von Blockchain für das SCM im Speziellen in drei Felder differenzieren lassen:

- Optimierung des internationalen Warenaustauschs und deren Dokumentation
- Rückverfolgbarkeit von Frachtträgern und Produkten bzw. Rohstoffen
- Echtzeit-Lokalisierung von Produkten innerhalb ihrer Lieferkette

Diese drei Anwendungsfelder werden nachfolgend vorgestellt und jeweils anhand eines Anwendungsbeispiels erläutert.

1) Optimierung des internationalen Warenaustauschs und deren Dokumentation

Gerade im internationalen Handel mit einer Vielzahl von Akteuren sind die Anforderungen an die begleitende Dokumentation zum Warentransfer aufwendig und auch heute noch von

papierlastigen Prozessen geprägt. Dabei speichern die involvierten Partner einer Lieferkette jeweils für sie relevante Informationen auf ihren eigenen Datenbanklösungen und Speichermedien. Es entsteht eine **silohafte** Mehrfachspeicherung von Informationen bei den beteiligten Akteuren (Hinckeldeyn 2019). Prozesszeiten werden durch sich wiederholende Dokumentationskontrollen erhöht und Overhead-Kosten in die Höhe getrieben. Hier greift ein wesentliches Argument von Blockchain-Technologie. So könnten Informationen manipulationssicher und vertrauenswürdig zwischen Partnern ausgetauscht werden und Datenabgleich bzw. -kontrollen teils automatisiert werden. Alle Teilnehmer eines Supply Chain Netzwerkes nutzen dazu ein und dasselbe Speichermedium – die Blockchain. Die Echtheit von Dokumenten kann dabei mit der charakteristischen Manipulationssicherheit der Blockchain-Technologie sichergestellt werden. Nachträgliche, fälschliche Veränderung, bspw. an Frachtdokumenten im internationalen Handel mit einander unbekanntem, nicht vertrauenswürdigen Partnern sind dabei technisch nicht möglich (Leong et al. 2018; Wu et al. 2017).

Basierend auf diesen Vorteilen von Blockchain bei der Anwendung im internationalen Warenaustausch ist **TradeLens, ein Joint Venture von IBM und Maersk** – seit Dezember 2018 mit kommerzieller möglicher Nutzung – als relevantes Anwendungsbeispiel zu nennen. Es handelt sich dabei um eine Blockchain-Plattform für alle Akteure, die in der Logistik von Seefracht-Containern involviert sind. Berücksichtigt werden dabei Reedereien, Häfen und Containerterminals sowie Zollbehörden und Speditionen, die über die bereitgestellte Plattform die jeweils notwendigen Daten für einen internationalen Warentransport per Frachtschiff austauschen. Technisch basiert die Plattform dabei auf Hyperledger Fabric, sodass nur ausgewählte Teilnehmer, nach vorangegangener Prüfung über die Plattform interagieren können. Die Anwendung von Smart Contracts findet sich dabei in sog. „Tradelens Business Funktionen“ wieder. So werden bspw. Zollmeldungen bei dem Eintreffen entsprechender Voraussetzungen **automatisiert** ausgelöst (Tradelens 2018).

Anfang 2019 nutzen bereits über 120 Unternehmen die Blockchain-Lösung im internationalen Seefracht-Transport. Dabei werden täglich über 1,5 Mio. Ereignisse von insgesamt 20 Mio. bekannten Containern aufgezeichnet. Der Datenaustausch zwischen den Playern beschränkt sich derzeit auf drei Datentypen (Tradelens 2018; Hinckeldeyn 2019):

- 1) Import- bzw. Exportdokumente in digitalisierter Form für schnellere Zollprozesse
- 2) Information über den Fortschritt eines Transportauftrags anhand sog. Meilensteine, die nach Ausführung bestimmter Aktionen als erreicht gelten
- 3) Verarbeitung von Sensordaten liefert Informationen über Warenzustand

Technisch lässt sich die Tradelens-Plattform dabei in Form eines Schichtenmodells nachvollziehen. In der ersten Ebene setzt sich das Netzwerk der Teilnehmer zusammen. Diese

müssen sich einer Prüfung unterziehen, bevor sie dem Netzwerk beitreten können. Über eingerichtete Kanäle können die registrierten Akteure Informationen auf der Plattform veröffentlichen und empfangen. Die Informationen werden dabei auf einer Hyperledger Fabric Blockchain abgespeichert. Datensätze, die in einem Kanal zwischen Nutzern geteilt werden, sind außerhalb dieses Kanals nicht sichtbar. Die dritte Ebene kann dabei als ‚Marktplatz‘ verstanden werden. Auf diesem ‚Marktplatz‘ werden Anwendungen angeboten, die Tradelens oder Netzwerkteilnehmer einbringen können (Hinckeldeyn 2019).

Größte Kritik an der TradeLens-Lösung wird immer wieder in der Macht von IBM und Maersk gesehen, die jeweils zu 50 Prozent die Leitung des Projektes übernehmen. Gerade Reedereien und Logistiker stehen dem Modell kritisch gegenüber, so arbeiten bspw. Kühne + Nagel zusammen mit Accenture und APL an einer alternativen Lösung. Hapag-Lloyd und CMA CGM haben sich ebenfalls nicht angeschlossen. Vor dem Hintergrund stellt sich die Frage, inwieweit TradeLens zukünftig das volle Potenzial einer vertrauenswürdigen Plattform im internationalen Warenaustausch ausschöpfen kann, wenn nicht alle relevanten Player involviert sind.

2) Rückverfolgbarkeit von Frachträgern und Produkten bzw. Rohstoffen

Bereits die Marktanalyse bestehender Pilotprojekte im Agrar- und Lebensmittelsektor hat gezeigt, dass offensichtlich ein großes Potenzial in der Anwendung von Blockchain für die Nachverfolgung von Produkten bzw. Objekten in ihrer Lieferkette gesehen wird. Andere Branchen, wie die Automobilindustrie oder die Bekleidungsindustrie beschäftigt sich in Pilotprojekten ebenfalls mit diesem Anwendungsfall. Zwei Anwendungsbeispiele veranschaulichen die Potentiale von Blockchain dabei leicht nachvollziehbar:

a) GS1-Pilotprojekt zum Palettentausch auf einer Blockchain

Im Rahmen eines Pilotprojektes hat sich ein Konsortium aus über 35 Partnern unter der Leitung der GS1 Germany GmbH zusammengeschlossen, um die Potenziale von Blockchain beim Austausch von Paletten als Frachträger zu erproben. Zu den Playern gehörten u.a. Markant, Kaufland, Dole Europe, Dr. August Oetker Nahrungsmittel KG, Lekkerland, Metro, Mars Holding, Wernsing Food Family und Spar Österreichische Warenhandels AG. Weitere Partner aus der Logistikbranche, IT, Beratung und FMCG waren ebenfalls involviert. Der Prozess des Palettentauschs wurde bewusst ausgewählt, da er heute als extrem papierlastig charakterisierbar ist. Dabei ist eine Vielzahl von Akteuren beteiligt, die einander meist nicht kennen. Nach Schätzungen ist laut des Projektträgers davon auszugehen, dass allein in Europa ca. 500 Mio. Paletten in Nutzung sind, wodurch sich ein Wert von 2,5 Mrd. Euro ergibt. Durchschnittlich fünf Umläufe absolviert eine Palette pro Jahr, sodass sich Prozesskosten i.

H. v. 9,5 Mrd. Euro ergeben. Der entwickelte Prototyp zur Erprobung von Blockchain-Technologie im Projekt umfasst drei Elemente:

- Mobile App für Logistik-Mitarbeiter am Ort des Geschehens
- Verwaltungsportal mit Bearbeitungsmasken für administrative Prozesse
- MultiChain-Blockchain Netzwerk mit 13 Knotenpunkten und 17 Teilnehmern an 20 Standorten

Während der 14-tägigen Umsetzungsphase wurden rund 600 Palettenübergänge aufgezeichnet. Zudem fand ein Belastungstest statt, indem 3.600 Transaktionen in einer Stunde absolviert werden konnten.

Das Fazit der Projektteilnehmer ergab zwar ein grundsätzlich positives Gesamtbild. Dennoch waren sich alle Teilnehmer darüber einig, dass die realisierten Anwendungen auch ohne eine Blockchain möglich gewesen wären. Generell konnte die Prozesseffizienz in Administration und Wareneingangs- und -ausgangslager gesteigert werden, während die Betriebskosten der Blockchain-Lösung übersichtlich geblieben sind. Der Aufbau des Netzwerks zu Beginn hat einen der Hauptkostentreiber dargestellt. Ebenfalls stellte sich die Entwicklung eines gemeinsamen Standards sowie die Inbetriebnahme des entwickelten Systems als herausfordernd dar. Die Störanfälligkeit während der Nutzungsphase war dabei gering. Als große Herausforderung wurde von den Teilnehmern der steigende Speicherplatz gesehen. So entstünden bei 3.600 Tauschvorgänge/h rund 200 GB Daten pro Jahr. Kritisch wurde zudem der unabdingbar zuverlässige Internetzugang bei allen involvierten Punkten gesehen.

Alles in allem wird die Technologie von den Teilnehmern **als „Katalysator“ für eine stärkere Kollaboration** gesehen, gerade vor dem Hintergrund, dass Transparenz und Datenschutz / Privatsphäre so stark im Kontrast stehen und die Bereitschaft zum Teilen von Informationen, selbst bei Frachträger-Daten für die meisten Teilnehmer eingangs sehr kritisch eingeschätzt wurde. Mittels der Erprobung einer Blockchain-Anwendung wurden diese Vorbehalten hinsichtlich einer stärkeren Kollaboration minimiert (GS1 Innovation 2018).

b) IBM Food Trust zur schnellen Rückverfolgbarkeit von Lebensmitteln

Für die Herkunft von Lebensmitteln gibt es neben der Lösung von IBM noch etliche andere Anbieter und Pilotprojekte, die hierfür die Potenziale von Blockchain erproben und bereits kommerziell nutzen. Die FAO ist im Rahmen einer entsprechenden Studie dabei zu dem Ergebnis gekommen, dass die Blockchain Technologie die Verknüpfung von Lebensmittel und Prozessinformationen unveränderbar und manipulationssicher herstellen kann, wie es bisher keine technologische Lösung abbilden konnte (Tripoli und Schmidhuber 2018). Walmart veranschaulichte an einer Mango in einem ersten Pilotprojekt mit IBM bereits 2017, dass die schnelle Rückverfolgbarkeit mittels Blockchain-Technologie möglich ist. Daraufhin hat

Walmart ein Konsortium initiiert bei dem Player, wie Unilever, Nestlé, Mc Cormick and Co. und Tyson Foods die Identifikation verunreinigter Lebensmittel zusammen mit IBM weiter erprobt haben. Aus diesem Zusammenschluss entstand das seit Oktober 2018 kommerziell nutzbare IBM Food Trust. Zu diesem Zeitpunkt ist u.a. der europäische Einzelhandelsplayer Carrefour in die Plattform eingestiegen (IBM Food Trust 2019).

Als Value Driver des IBM Food Trust Plattform wird in erster Linie die Möglichkeit zur Effizienzoptimierung in komplexen Lieferketten mit einer Vielzahl von Playern gesehen. Hersteller haben laut IBM so zudem die Möglichkeit, ihren Markenwert durch Verbrauchervertrauen in die entsprechenden Marken auszubauen, da Lebensmittelsicherheit und Rückverfolgbarkeit im Krisenfall schnell abbildbar sind. Datenanalysen geben zudem Aufschluss über Produktfrische und Inventurbestände und können so Lebensmittelverschwendung reduzieren und Lagerprozesse optimieren. Die Möglichkeit, Zertifizierungsdokumente, Lizenzen und Prüfergebnisse in der Plattform einzuspielen, schafft einen Betrugsschutz und kann zudem die Nachhaltigkeitsbedingungen in einer Lieferkette belegen. IBM Food Trust setzt sich auf Nutzerebene dabei aus verschiedenen Anwendermodulen zusammen, die in der folgenden Tabelle in Kürze beschrieben sind.

Tab. 7: Module des IBM Food Trust Systems (IBM Food Trust 2019)

Trace	<ul style="list-style-type: none"> • Rückverfolgbarkeit und Produktherkunft f. autorisierte Teilnehmer • Echtzeitinformation über Produktstatus und -standort • Möglichkeit des Rückrufs mittels GTIN, Produktname, Lieferscheine • Je nach Nutzer kann auch nur begrenzter Zeitraum einsehbar sein
Fresh Insights	<ul style="list-style-type: none"> • Analysetool von Produktdaten zur Ableitung von Inventaroptimierung • Möglichkeit, Messwerte verschiedener Standorte zu vergleichen • Verweilzeiten von Produkten an einem Standort • Berechnung Ablaufdatum, Produktionsdatum • Berechnung von Risikoinventar • Optimierung der Produktfrische und Reduktion von Produktverlusten • Optionale Verknüpfung mit IoT-, RFID usw. für weitere Analysen
Certification	<ul style="list-style-type: none"> • Digitalisierung von Zertifikaten, Prüfdokumenten, Lizenzen usw. • Steigerung der Effizienz im Dokumentenmanagement • Ausgewählter „Certification Manager“ für Upload und Management der gültigen Lizenzen und Ergebnisdokumente
Data Entry And Access	<ul style="list-style-type: none"> • Jeder bleibt Besitzer seiner Daten und vergibt ausgewählte Leserechte / Informationen an andere autorisierte Teilnehmer • Möglichkeit des automatisierten Datenimport von externen Systemen ist möglich (z. B. SAP o.Ä.)

IBM Food Trust basiert wie TradeLens auf einer Hyperledger Fabric Blockchain und bildet aus den Nutzern des Systems die gemeinsame IBM Blockchain Plattform. Auf dieser Plattform

werden verschiedene Systemlösungen für die Anwender angeboten. Dazu zählen die in der obenstehenden Tabelle genannten Module sowie der Onboarding Service neuer Teilnehmer durch IBM und ein Bereich für die Entwicklung neuer Tools. In gleichem Prinzip wie bei Tradelens, können auch bei Food Trust Informationen in Kanälen zwischen Teilnehmern ausgetauscht werden, ohne dass es Nutzer außerhalb des entsprechenden Kanals einsehen können. Hinzu kommt die Verwendung von Smart Contracts, die ebenfalls fallbezogen in einem solchen Kanal zwischen ausgewählten Geschäftspartnern aufgesetzt werden können (IBM Food Trust 2019).

3) Echtzeit-Lokalisierung von Produkten innerhalb ihrer Lieferkette

Im Zusammenhang mit dem Supply Chain Management ist die Lokalisierung eines Transportgutes und die Aufzeichnung des Standortverlaufs von Produkten ein häufig genanntes Paradebeispiel, wenn die Anwendungsfelder von Blockchain diskutiert werden (Lin et al. 2018; Leong et al. 2018; Tian 2016). Um den Standort eines Produktes eindeutig identifizieren und nachverfolgen zu können, braucht es sog. Location-Based-Services. GPS-Sender können über die Zuordnung von Koordinaten diesen Service bspw. sicherstellen (Hinckeldeyn 2019). Dabei weisen GPS-Lösungen jedoch technische Herausforderungen auf. So handelt es sich um ein System, das zentral organisiert ist und bei einem entsprechenden Systemausfall in Gänze betroffen sein kann. Die Identifikation von Koordinaten kann innerhalb von Gebäuden oder unterirdisch problematisch sein. Zudem handelt es sich um ein unverschlüsseltes Protokoll, das einfach manipuliert werden kann. Stand heute mangelt es an einem Verifizierungssystem von aufgezeichneten GPS-Daten (Hinckeldeyn 2019; Kandel et al. 2011).

Ein Anwendungsbeispiel, bei dem Blockchain zur Echtzeit-Lokalisierung von Gegenständen genutzt wird, ist ein Konzept des Start-ups FOAM. Hierbei handelt es sich um ein Blockchain-Protokoll, das einen **Proof-of-Location** erstellt, um ein resilienteres System zu realisieren, mit dem Standorte unabhängig von GPS-Daten definiert werden können. Neben der Blockchain-Technologie wird die sog. Low-Power Long Range Spread-Spectrum Funktechnologie (LoRa) verwendet. Mittels LoRa-getriebener Netzwerkknoten können Gebäude oder Straßenverläufe lokalisiert werden, ohne dass es der Nutzung von GPS-Daten bedarf. Hauptantrieb für die Entwicklung eines standort-verifizierenden Konsens-Protokolls lag in der Anforderung, dass Smart Contracts für bestimmte Standorte eine Verifikation über die tatsächliche Erreichung / Vorhandensein an einem bestimmten Ort erfordern. Mit dem FOAM-Protokoll lassen sich entsprechende Orte in Echtzeit entsprechend verifizieren. Beim sog. Proof-of-Location lässt sich also mittels Konsens feststellen, ob ein Status zu einem bestimmten Zeitpunkt am vorgegebenen Ort tatsächlich eintritt. Grundsätzlich wird **FOAM** für

Anwendungen im Supply Chain Management, im Bereich des autonomen Fahrens und der Beobachtung von Verkehrsflüssen gesehen. Zwar befindet sich FOAM aktuell noch in der Entwicklungsphase und kann noch keine Prototypen oder Pilotprojekte verzeichnen. Unter Berücksichtigung bisheriger Publikationen ist das Protokoll aber weiter zu beobachten. So könnte das Konzept den Markt für Geodaten verändern, da ein deutlich sichereres und widerstandsfähigeres Konzept mit FOAM möglich sein könnte. Ebenfalls sehen die Entwickler neben dem Anreizsystem – nämlich bei der Bereitstellung von Knotenpunkten Mikrozahlungen zu erhalten – einen Markt in der Veräußerung von privat aufgezeichneten, betrugssicheren Standortdaten (Schiller 2018; Foamspace Corp 2018).

2.2.1.3 Herausforderungen von Blockchain im Supply Chain Management

- Schnittstelle reale Welt / digitale Welt nicht immer sicher
- Einmal eingespeicherte Daten nicht veränderbar / löschar (Datenschutz)
- Bisher liegt „Macht“ von Systemen bei zentralen Einheiten (IBM), tatsächliche Dezentralität in Governance stellt sich schwierig dar
- Private bzw. Konsortiale Blockchains, wo eigentlicher Gedanke des Wegfalls von Intermediären übergangen wird
- Speicherkapazität, da Blockchain immer weiterwächst
- Paradigmenwechsel zum Teilen von Daten nötig
- Ein Stück weit muss Vertrauen zwischen Akteuren bereits herrschen, um überhaupt in einem solchen Netzwerk zusammenzuarbeiten bzw. Lieferbeziehungen einzugehen

2.2.2 Auditierung und Zertifizierung

Unabhängig von der Agrar- und Lebensmittelbranche und derzeit noch mit wenigen Pilotprojekten vertreten, aber dennoch theoretisch diskutiert, ist das Anwendungsfeld der (Nachhaltigkeits-) Auditierung und Zertifizierungen. Welches im folgenden Abschnitt ebenfalls in Kürze nach den Unterpunkten: heutige Problemstellungen, Lösungspotenziale und Anwendungsbeispiele von Blockchain sowie technische Grenzen vorgestellt wird.

2.2.2.1 Aktuelle Problemstellungen

Grundsätzlich lassen sich im Bereich der Auditierungen und Zertifizierung von Managementsystemen, Produktionsverfahren und Lieferanten heutige Herausforderungen in die folgenden Bereiche unterteilen.

a) Erwartungshaltung Transparenz

Skandale über Produktionsbedingungen oder Verunreinigungen sowie die Diskrepanz zwischen der Verbrauchervorstellung und realen Produktionsabläufen haben dazu geführt, dass heute zum einen eine gestiegene Erwartungshaltung gegenüber der Transparenz und zum anderen Unsicherheit bezüglich der Glaubwürdigkeit von Informationen über

Produktherkunft, verwendeter Materialien und Einhaltung von (Nachhaltigkeits-)standards bei Konsumenten vorherrscht (Schwarzkopf et al. 2018).

Aus Unternehmenssicht führt die Komplexität heutiger Lieferketten ebenfalls zu einem Mangel an Transparenz und Glaubwürdigkeit in die anderen Akteure einer involvierten Supply Chain. So verfügen Unternehmen zwar über die Zertifizierungs- bzw. Auditierungsinformationen ihrer direkten Zulieferer und ggf. auch ihrer weiterverarbeitenden Kunden, häufig aber nicht über die Einhaltung entsprechender Standards bei Sub-tier-Lieferanten. Gerade in internationalen Lieferketten mit einer Vielzahl an Zulieferern steigt somit der Vertrauensanspruch in den jeweils vorgelagerten Lieferanten und seine Überprüfung der Anforderungen bei den entsprechenden Zulieferern der Vorstufe (z. B. Müller und Bessas 2017).

b) Ineffizienzen in Kontrollprozessen / Doppelauditierungen

Mitunter getrieben durch die mangelnde Transparenz und Glaubwürdigkeit zwischen Lieferkettenakteuren, wird die Einhaltung entsprechender Branchen- und Nachhaltigkeitsstandards durch unabhängige Prüfgesellschaften in definierter Regelmäßigkeit kontrolliert und zertifiziert. Da ein Unternehmen i. d. R. mehr als einen Kunden auf der nächsten Stufe der Wertschöpfungskette beliefert, muss sich ein Unternehmen meist auch mehreren Standards und entsprechenden Auditierungen unterziehen. Die Intransparenz zwischen den unterschiedlichen Systemen führt dazu, dass von unterschiedlichen Prüfgesellschaften / Auditoren innerhalb kürzester Zeit in einem Betrieb mehrere Audits durchgeführt werden. Die Doppelauditierungen führen zu Ineffizienzen im zu prüfenden Betrieb und in den Zertifizierungsgesellschaften. Gleichzeitig tritt so das Problem auf, dass ein Betrieb möglicherweise in kürzester Zeit mehrfach an ähnlichen Kontrollpunkten bewertet wird und Problemherde dabei ggf. unentdeckt bleiben. In dieser Systematik können indes Unternehmen mit einer schlechteren Performance gleichzeitig über längere Intervalle mit bestehender Zertifizierung und Zulassung in der Lieferkette interagieren, bevor es im Folgeaudit auffällt (Müller und Bessas 2017, Schwarzkopf et al. 2018).

c) Betrugs- und Fälschungsrisiken

Branchenunabhängig liegt eine weitere Herausforderung im Umgang und der Identifizierung mit gefälschten oder manipulierten Zertifizierungsdokumenten und Prüfergebnissen. Gerade im internationalen Kontext ist die Kontrolle über die Echtheit eines Zertifikates teils nur schwer abbildbar und erfordert aufwendige administrative Prozesse. Bei der Auditierung durch unabhängige Prüfgesellschaften kann je nach Zielregion das Problem der Korruption eine Diskrepanz zwischen Auditergebnis und tatsächlicher Situation hervorrufen. Eigens durchgeführten Lieferantenaudits können dem zwar vorbeugen, ziehen aber hinsichtlich der nötigen Ressourcen entsprechende Ineffizienzen mit sich. Im Falle eines Skandals innerhalb

eines zertifizierten Betriebes (z. B. Umgang mit Schlachtvieh, Lebensmittelverunreinigungen, Produktionsbedingungen Textilindustrie usw.) kann zudem die Glaubwürdigkeit des entsprechenden Standards gefährdet werden und die nachträgliche Manipulation von vorangegangenen Kontrollen zum Imageschutz von Zertifizierungsgesellschaft oder Standard niemals endgültig ausgeschlossen werden (Eickmeyer et al. 2018).

2.2.2.2 Lösungspotenziale und Anwendungsbeispiele

Die Anwendung von Blockchain in diesem Feld verspricht v. a. eine **erhöhte Fälschungssicherheit** und damit verbundene Authentizität aufgrund der dezentralen Datenbankstruktur und Kryptographie. Bei der **Speicherung von Hash-Werten** kann dabei ein **datenschutz-konformer Umgang mit vertraulichen Daten** realisiert werden. Die Speicherung in verteilten Netzwerken schafft einen **neuen Grad an Transparenz**, wodurch Vertrauen gesteigert werden kann und Effizienzpotentiale genutzt werden können. Darüber hinaus kann mithilfe der Blockchain-Technologie allein deshalb ein **vertrauenswürdiges Image** geschürt werden, da mit ihr als innovative Lösung ein hohes Maß an Transparenz und Manipulationssicherheit assoziiert wird (Hosp 2018). Die in Kapitel 1.2 beschriebenen Funktionsweisen von Smart Contracts schaffen darüber hinaus Ansatzpunkte für die Automatisierung von Prozessen, in denen es heute noch administrative Ressourcen zur Überprüfung der Dokumentenechtheit bedarf.

Das Potenzial von der Verknüpfung mit Sensortechnik und sich damit verändernden Prüfmechanismen wird in Kapitel 2.2.3 detailliert betrachtet, während dieses Kapitel eher den Umgang mit Zertifikaten, deren Gültigkeit und Auditergebnisdokument umfasst.

Ein Anwendungsbeispiel aus dem Bereich des Personalmanagements

Anwendungsbeispiel Certivation: Das deutsche Start-Up hat eine Lösung entwickelt, mit der Abschlusszeugnisse manipulationssicher und im Rahmen der DSGVO-Anforderungen in einer dezentralen Systematik gespeichert und von betroffenen Parteien abgerufen werden können. Bildungseinrichtungen können dazu entsprechende digitale Zertifikate einzeln oder als Massenupload von Teilnehmern und Absolventen in die Blockchain hochladen. In der Blockchain wird damit ein entsprechender Eintrag in Form eines Hashwertes erstellt. Bildungseinrichtung und Teilnehmer erhalten ein Blockchain-Zertifikat mit zwei QR-Codes, die den Zugriff auf den Eintrag und damit das Zeugnis erlauben und diesen mit potentiellen Arbeitgebern im Bewerbungsprozess teilen können. In diesem Prozess wird eine aufwendige Echtheitsprüfung von Zeugnissen eines Bewerbers im Grunde überflüssig. Für Absolventen wird eine amtliche Beglaubigung von entsprechenden Dokumenten ebenfalls hinfällig. Certivation nutzt dazu eine offene Ethereum-Blockchain (Certivation GmbH 2019).

Zwar entstammt das beschriebene Anwendungsbeispiel aus dem Bereich des Personal-Recruitings, bietet aber dennoch Ansatzpunkte, die auch im Bereich der Zertifizierung und Auditierung von Produktionsabläufen oder Lieferanten sinnvoll sein können. Gerade mit Blick auf internationale Akteure aus Ländern mit schlechten Korruptionsindex (CPI) bietet dieser Ansatz Sicherheit im Umgang mit Prüfdokumenten und Zertifikaten. Die IBM Food Trust Plattform bietet bereits diesen Service an, die manipulationssichere Speicherung von Zertifikaten auf Blockchain-Basis (IBM Food Trust 2019).

2.2.2.3 Herausforderungen von Blockchain in der Auditierung und Zertifizierung

- Schnittstelle zwischen physischer Welt und Datenbank ist weiterhin manipulations- und fehleranfällig.
- Möglichkeit der Manipulation besteht auch weiterhin **vor** der Dateneingabe in System.
- Prinzip der Netzwerkökonomie: System bietet erst Mehrwert, wenn möglichst viele Akteure Zertifikate bzw. Auditergebnisse speichern.
- Skepsis ggü. dezentraler Speicherung vertraulicher Daten, kann eine solche Lösung hemmen, wenngleich dies technisch möglich ist.
- Investition und Aufbau einer Governance-Lösung zu Beginn eines Blockchain-basierten Systems sind hoch und weniger planbar als zentrale Lösungen.

2.2.3 Internet der Dinge (IoT)

Der Anwendung von Blockchain in Verbindung mit bereits bestehenden Lösungen aus dem Feld der IoT-Technik gilt verschiedenen Studien zufolge als eines der bedeutsamsten Felder für Blockchain (Sallaba et al. 2018; Lin et al. 2018; Schütte et al. 2017). Auch in Lieferketten von Lebensmitteln finden sich IoT-Lösungen zur Kontrolle von Kühlketten oder der Einhaltung von Lieferrouten oder bspw. hinsichtlich der Wartung von Fertigungsmaschinen wieder. Auch in der Landtechnik-Branche wird an IoT-Lösungen zur direkten Interaktion zwischen Maschinen gearbeitet (Lin et al. 2018). Gerade mit Blick auf das vorangegangene Anwendungsfeld der Auditierung kann IoT in Verbindung mit Blockchain eine gänzlich neue Relevanz für Lebensmittellieferketten erhalten.

2.2.3.1 Aktuelle Problemstellungen

Das Erfassen und Austauschen von Sensordaten innerhalb einer Lieferkette unmittelbar zwischen einzelnen smarten Maschinen stellt nicht nur für die Lebensmittelindustrie ein Kernthema der Digitalisierung dar. Auch für die Urproduktion beschäftigt sich die Landtechnikbranche mit zunehmend vernetzten Lösungen zwischen einzelnen Maschinen und automatisierten Entscheidungsprozessen auf Basis von umfangreichen Datengrundlagen (Horstmann 2015). Das Internet der Dinge (IoT) liefert dabei essentielle technologische Werkzeuge für die Vernetzung von Maschinen und Produktionsstandorten und der

Aufzeichnung entsprechender Datensätze. Liefern IoT-Services zwar immer neue Möglichkeiten für effizientere Prozesse und Automatisierung, liegt die wesentliche Gefahr im Vertrauen und der Kontrolle solcher direkt miteinander verbundenen Maschinennetzwerke. Kann man solchen Systemen vertrauen und wenn ja wie? (Hosp 2018). Ähnlich wie bei den oben beschriebenen GPS-Lösungen ist die nachträgliche Fälschungssicherheit und der Ausfall einer zentralen Speicherlösung dabei nicht ausgeschlossen (Sallaba et al. 2018). Gerade beim Austausch von Sensordaten außerhalb des eigenen Unternehmens herrscht Skepsis hinsichtlich der Datensicherheit (Lin et al. 2018).

2.2.3.2 Lösungspotenziale und Anwendungsbeispiele

IoT-Sensortechnik und die Rückverfolgbarkeit von Lebensmitteln geht in der wissenschaftlichen Theorie und in untersuchten Pilotprojekten eng miteinander einher (Caro et al. 2018; Lin et al. 2018; Sallaba et al. 2018; Carbone et al. 2018). Wo es bisher zu den oben beschriebenen Herausforderungen von IoT-Lösungen keine Ansatzpunkte für den sichereren Datenaustausch und die Verifizierung von Dateninput gibt, kann Blockchain der dritten Generation, wie bspw. IOTA entsprechende Lösungsansätze bieten. Zum einen wird die Schnittstelle zwischen physischer und digitaler Welt mit verifizierten Sensoren gesichert und die Speicherung der erfassten Daten mit den Vorzügen der Blockchain-Technologie realisiert. Der sichere Austausch von produktionsrelevanten Daten kann innerhalb eines verteilten Netzwerkes ebenfalls abgebildet werden. Im Grunde schafft eine Symbiose von IoT-Lösungen und Blockchain die notwendigen Voraussetzungen für eine lückenlose, transparente und dennoch sichere Rückverfolgbarkeit von Lebensmitteln über eine komplexe Lieferantenstruktur hinweg (Caro et al. 2018). Damit kann das Vertrauen in IoT-Lösungen erhöht werden und ein vernetztes System unterschiedlicher Geräte und Sensoren vor Hackerangriffen geschützt werden (Hosp 2018). Verschiedene Startups setzen auf der Kombination dieser beiden innovativen Technologien an.

Anwendungsbeispiel ‚Ripe.io‘ und ‚Hyperledger Sawtooth‘: In einem Pilotprojekt mit Sweetgreen Inc., einem Franchise-Systemanbieter für Salate in den USA und einem 180 Hektar großen Gemüsebetrieb hat das Startup Ripe.io die Kombination von Sensortechnik und einer Blockchain-Plattform erprobt. Dabei werden bei der Tomatenproduktion Licht, Luftfeuchtigkeit und -temperatur mittels solarbetriebener Sensoren erfasst und in einer Blockchain gespeichert. Neben dem Anbau, liefern Sensoren in Transport- und Lagerbehältnissen Informationen über die Luftfeuchtigkeit während der Lagerungsprozesse. Darüber hinaus werden Reifegrad, Farbe und Zuckergehalt der Tomaten dokumentiert (Whalley 2018).

Ein weiteres Anwendungsbeispiel basiert auf einer Weiterentwicklung der Hyperledger Foundation in Kooperation mit Intel. Mit der sog. Hyperledger Sawtooth Plattform wurde eine

Blockchain-Lösung geschaffen, die sich für die Rückverfolgbarkeit in Lebensmittellieferketten durch Integration von IoT-Sensortechnik anbietet. Das Sawtooth-Design basiert dabei auf dem eigens entwickelten Konsensmechanismus „Proof of Elapsed Time“ und erlaubt durch die Integration von Smart Contracts Möglichkeiten zur automatisierten Kontrolle von Produktbeschaffenheit an verschiedenen Produktionszeitpunkten sowie Regeln für Transaktionsprozesse. Pilotweise wurde die Lösung bereits an der Lieferkette von Fischereiprodukten getestet und Temperatursensoren zur Einhaltung von Kühlketten-Standards integriert. Ähnlich wie Hyperledger Fabric wurde auch Sawtooth als Blockchain Framework für Unternehmen entwickelt und hat nicht mehr viel Ähnlichkeit zu Blockchain-Lösungen für die Abwicklung von Kryptowährungen. Dabei umfasst Sawtooth einige Lösungsansätze, die beim Blockchain-Einsatz in Unternehmen zuvor als Herausforderungen deklariert wurden. Olson et al. (2018) fasst diese wie folgt, zusammen:

- Smart Contracts als Mittel einer On-Chain-Governance: Zugelassene Nutzer können bspw. mithilfe von Smart Contracts definiert und abgestimmt werden.
- Blockerstellung und -validierung und damit Transaktionsgeschwindigkeit wurde durch Konsensverfahren verbessert und erlaubt eine parallele Abwicklung von Transaktionen.
- Möglichkeit der Integration von Smart Contracts in Ethereum-Lösungen.
- Dynamische Entwicklung des Konsens-Protokolls während Sawtooth in Betrieb ist. So lassen sich skalierbare Algorithmen während des Netzwerkwachstums im System einfügen.
- Möglichkeit in verschiedenen Programmiersprachen, je nach Bedarf, neue Smart Contracts zu programmieren (Java, JavaScript, Python etc.).

Die nachfolgende Abbildung von Hyperledger Sawtooth (2018) veranschaulicht dazu die Möglichkeiten der Sensorintegration im Hyperledger Sawtooth Framework am Beispiel von Seafood Supply Chain Traceability.

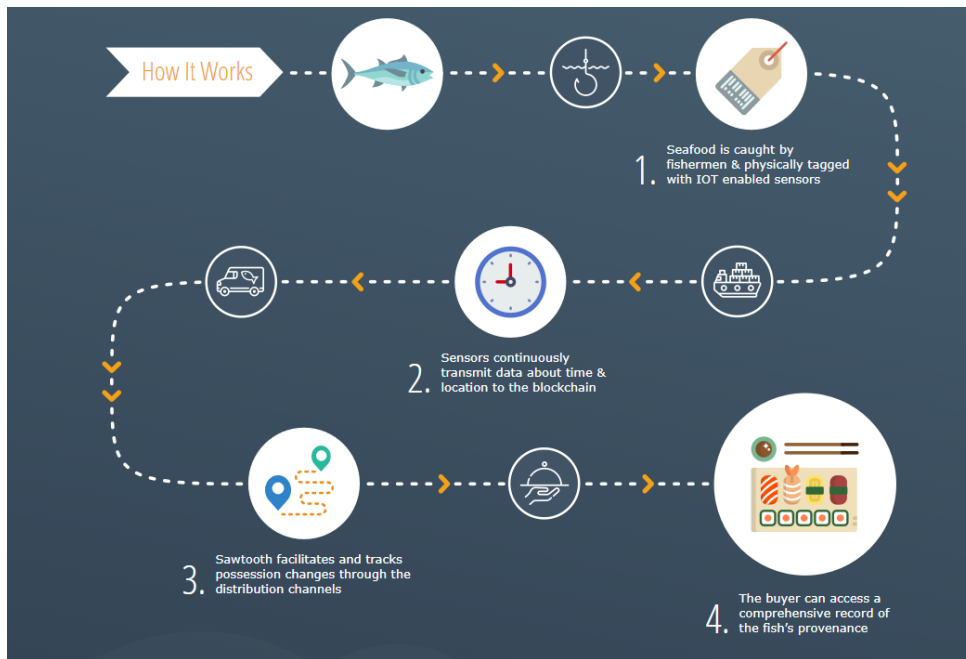


Abb. 11: Sawtooth für Seafood Supply Chain Traceability (Hyperledger Sawtooth 2018)
 Zahlreiche weitere Projekte nutzen die Anwendung von IoT-Lösungen in Kombination mit der Blockchain-Technologie für die Rückverfolgbarkeit von Lebensmitteln in ihrer Supply Chain (siehe Anhang 1). So arbeitet bspw. das australische Start-Up Beefledger an einer entsprechenden Integration von Sensortechnik (siehe Anhang 1).

2.2.3.3 Herausforderungen von Blockchain in Verbindung mit IoT-Lösungen

- Dezentralität bringt Fragen hinsichtlich der Verantwortlichkeit für das System. Wenn keine zentrale Instanz die Vernetzung der Maschinen und Geräte kontrollieren kann, wer greift dann im Falle eines Maschinenfehlers ein bzw. ist für Folgen verantwortlich?
- Beispiele haben gezeigt, dass IoT-Systeme auf Blockchain-Basis in einem Maße dezentralisiert werden können, dass die Entwickler selbst nachträgliche Programmierungsfehler (Bugs) nicht mehr korrigieren können. Ein Beispiel: Ein Startup entwickelte smarte Thermostate auf Blockchain-Basis, um Manipulation komplett auszuschließen. Während der Programmierung wurde eine Möglichkeit für einen Hackerangriff übersehen und dieses später ausgenutzt. Der Erpresser stellte das Thermostat so ein, dass sich bis zur Lösegeldzahlung an eine Kryptoadresse des Hausbesitzers die Temperatur stündlich erhöhte. Nachträglich konnte der Hack von niemandem korrigiert werden, sodass die einzige Lösung die Zerstörung des Thermostats war (Hosp 2018).

3 Hypothesen zur Relevanz von Blockchain für Lieferkette-Akteure

Das folgende Kapitel erläutert Hypothesen über die Bedeutung der Blockchain-Technologie für verschiedene Akteure innerhalb von Lebensmittel-Lieferketten. Die Ableitung dieser Hypothesen basiert auf der umfangreichen Sekundärdatenanalyse, deren Ergebnisse in den vorangegangenen Abschnitten bereits erläutert wurden. Eine wissenschaftliche Hypothesenüberprüfung in Form von qualitativer Primärdatenerhebung und -auswertung wird hierbei nicht mehr vorgenommen. Lediglich einzelne Gespräche mit relevanten Akteuren der Branche konnten die generierten Hypothesen bestätigen bzw. konkretisieren.

3.1 H1: Form des Vertrauens in abgespeicherte Daten verändert sich durch Blockchain-Lösung

Bald jede Form wirtschaftlichen Handelns geht mit Transaktionen von Werten, Waren oder Informationen einher. Essentiell für solche Transaktionen ist dabei Vertrauen. Vertrauen muss dazu zwischen Unternehmen und gegenüber Konsumenten bei jeglicher Art der wirtschaftlichen Interaktion als Grundvoraussetzung vorhanden sein. Vertrauensstiftende Institutionen fungieren dazu heute als Vermittler, Bürgen oder standardgebende Systeme. Ein weiterer Treiber für den Aufbau von Vertrauen liegt in der Reputation. Neben direkten Erfahrungen, spielen hier Erfahrungswerte Dritter mit ein. Etablierte Prüf- und Zertifizierungssiegel schaffen ebenfalls Vertrauenswürdigkeit in ein Produkt oder ein Unternehmen. Manipulationen unter solchen Siegeln, medial als Skandal oft breit behandelt, können aber auch zu einer vorschnellen, generalisierten Verunsicherung der Verbraucher in einen Markenführer oder eine Branche führen (Düring und Fisbeck 2017).

Vertrauenswürdigkeit wird heute zunehmend auf Basis von Transparenz beurteilt (Klenk & Hoursch 2011). Nach Edelman (2018) liegt dieser steigende Anspruch auf Transparenz in erster Linie in zunehmend komplexer werdenden Wirtschaftsstrukturen, schnelleren Innovationszyklen und Globalisierung sowie Korruption und Manipulation. Nach Düring et al. (2017) kann Vertrauen erst dann in vollem Maße hergestellt werden, wenn entweder dokumentierte Transparenz oder aber die Möglichkeit der persönlichen Kontrolle bzw. des persönlichen Wissens über einen Zustand gegeben ist (siehe folgende Abbildung).

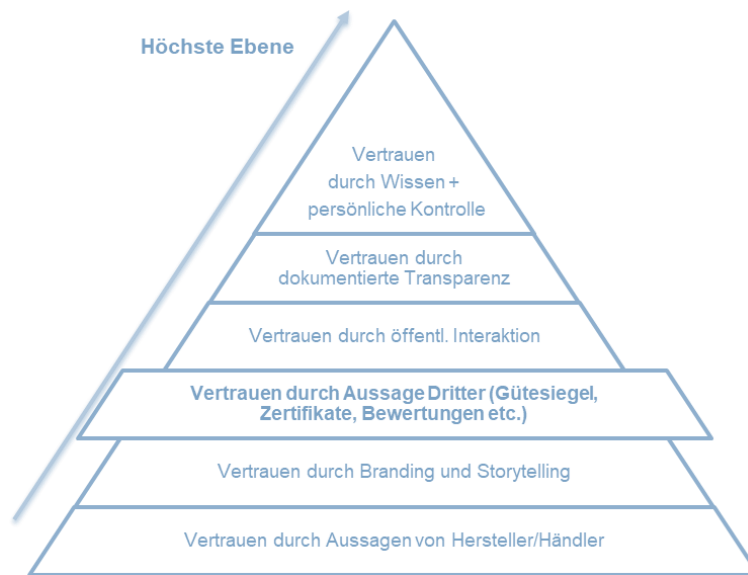


Abb. 12: Ebenen der Vertrauensbildung (Düring et al. 2017, S. 452)

Blockchain kann mit zwei Kerneigenschaften den steigenden Anforderungen an Transparenz begegnen. Zum einen erlaubt es die transparente Abbildung von Datensätzen, nahezu in Echtzeit, zum anderen sind Informationen chronologisch nachvollziehbar, ohne die Möglichkeit einer Löschung oder Manipulation einmal abgespeicherter Datensätzen. Mit dieser Form der Datensicherheit und -authentizität kann Vertrauen auf der Ebene der dokumentierten Transparenz geschaffen werden. Neben der inhaltlichen Integrität der Datensätze, bringt auch die eindeutige Identifikation der Teilnehmer sowie die Sicherheit des Systems ggü. Ausfällen oder Hackerangriffen die nötigen Anforderungen an eine vertrauenswürdige Technologie mit sich (Tapscott und Tapscott 2018).

Auf diese Weise schafft Blockchain eine technologische Möglichkeit, die Nachweisbarkeit in der Erzeugung von Lebensmitteln transparenter abzubilden und damit Glaubwürdigkeit zwischen Lieferanten und Abnehmern sowie bei Endverbrauchern zu steigern. Bei Lebensmittelverunreinigungen können Problemherde schneller identifiziert werden und Produkte gezielter aus dem Markt genommen werden. Durch die Unveränderbarkeit der abgespeicherten Daten schafft die Blockchain-Technologie zudem einen neuen Grad der Beweiskraft, wodurch wiederum Vertrauenswürdigkeit gefördert wird (Düring und Fisbeck 2017).

Es lässt sich also festhalten, dass mit der Abbildung von Lieferketteninformationen in einer Blockchain sowohl Beweiskraft und damit sicheres Wissen über Prozesse, Transaktionen etc. gegeben ist und die Art der Dokumentation zudem Transparenz über einzelne Unternehmen hinweg hergestellt werden kann. Das Vertrauen in die reine Aussage von Akteuren der Lieferkette wird auf diese Weise durch Transparenz und die Möglichkeit der eigenen Kontrolle ersetzt.

Mit Blick auf die Akteure von Lebensmittel-Lieferketten kann hierin ein entscheidender Punkt liegen, der für die Attraktivität der Technologie spricht: von der Urproduktion bis zur Auslieferung an eine LEH-Filiale lassen sich einzelne Prozessschritte eines Produktes in einem einzigen System durch verschiedene Teilnehmer abbilden, wobei Informationen dezidiert mit Zugriffsrechten nur einzelnen Akteuren zugänglich gemacht werden. Jeder Akteur kann dabei Eigentümer seiner generierten Datensätze bleiben und von „Mehrinformation“, die er preisgibt bspw. ggü. Kunden profitieren. Dennoch nutzen alle Akteure ein und dasselbe Netzwerk und speichern Daten nicht mehr auf unternehmenseigenen Servern silohaft ab. Durch die Art der Speicherung kann ein einzelner Akteur die Daten im Nachhinein nicht mehr verändern. Mit dieser Systematik kann neben Effizienz in erster Linie Vertrauen über die Stufen der Wertschöpfungskette hinweg transportiert werden.

3.2 H2: Manipulationssicherheit der BCT kann besonders für Echtheitsnachweise im asiatischen Markt interessant werden/sein

Die Anzahl an Patentanmeldungen zu Blockchain sowie die Investitionssummen in BCT-Lösungen im asiatischen Raum zeigen, dass hier ein hohes Interesse und offensichtlich großes Potential ggü. der Technologie gesehen wird. Alleine die beiden Online-Handelsriesen Alibaba (60) und JD.com (200) halten Stand 2018 zusammen 260 Blockchain-Patente (BTC ECHO 2019). Mit Blick auf die staatlich geförderten Projekte im Lebensmittel- und Pharmasektor wird deutlich, dass staatliche Instanzen in asiatischen Ländern in der Technologie eine Möglichkeit sehen, um Betrugs- und Manipulationsmöglichkeiten einzudämmen und Transparenz und damit verbundene Rückverfolgbarkeit in Lieferketten von Lebensmitteln und Medikamenten zu optimieren. Der Fokus der Projekte liegt dabei meist in der Steigerung der Lebensmittelsicherheit.

Ein zweites Anwendungsfeld von Blockchain, welches im asiatischen Raum für den Lebensmittelsektor relevant ist, ist der internationale Warenaustausch und v.a. der Export qualitativ hochwertiger Produkte nach Asien. Die Zahlungsbereitschaft der chinesischen Verbraucher für qualitativ hochwertige Lebensmittel aus Drittländern (Europa, Australien) ist bspw. ein wesentlicher Treiber (Kendall et al. 2019). Dabei sehen sich nach Asien exportierende Unternehmen immer wieder der Gefahr gegenüber, dass Plagiate ihrer Produkte mit minderer Qualität auf dem Zielmarkt den eigenen Markenwert gefährden. Zahlungsbereite Endkonsumenten können sich indes nicht sicher sein, ob das Produkt tatsächlich den Angaben der Etikettierung entspricht oder es sich um ein Plagiat handelt (Sanders 2006; Kendall et al. 2019). Use Cases, wie der des australischen Startups Beefledger haben gezeigt, dass Blockchain den Produzenten hier eine Möglichkeit bieten kann, Endkonsumenten die Echtheit der Produkte digital und über den gesamten Prozess hinweg nachweisen zu können. Damit kann der Markenwert im entsprechenden Zielmarkt ggü. Produkten, die diesen Zusatznutzen nicht liefern, nochmal gesteigert werden. Für die

exportierenden Unternehmen geht mit einer solchen Systematik zudem die Möglichkeit einher, im Falle eines belasteten Plagiaten nachweisen zu können, dass es sich um ein Produkt handelt, welches nicht aus dem Wertschöpfungsstrom des Unternehmens stammt und entsprechend ein Etikettierungsbetrug vorliegt (z. B. Beefledger 2018). Es braucht dabei keine vertrauenswürdige Instanz, von der die Daten zentral abgespeichert werden. Denn auch eine vertrauenswürdige, zentrale Instanz könnte die gespeicherten Daten im Nachhinein zentral manipulieren oder Opfer eines Hacker-Angriffs werden. Mit Blick auf die Manipulationssicherheit von Dokumenten, kann die verteilte Speicherung auch für Zollbehörden oder weitere involvierte Institutionen im Außenhandel für rechtliche Dokumente relevant sein.

3.3 H3: Hype um Blockchain unter Lebensmittelhändlern liegt im Interesse an maximaler Transparenz der Zulieferströme

Die Marktanalyse hat gezeigt, dass ein massives Interesse an der Technologie beim LEH liegt. Gerade in puncto Supply Chain Management und Rückverfolgbarkeit wird hier der größte Mehrwert in der Distributed Ledger Technologie gesehen. Häufig angeführtes Motiv des LEH für dieses Interesse ist die Möglichkeit der optimierten Rückverfolgbarkeit entlang der Lieferkette in Sekundenschnelle aufgrund transparenter Wertschöpfungs-systeme. Gerade im Krisenfall erlauben bisherige Lösungen dem LEH eine schnelle Reaktion und die Möglichkeit Ursachenherde zu identifizieren. Dennoch zeigen Projekte, wie die von Walmart, Albert Heijn oder Carrefour, dass der dezentrale / konsortiale Ansatz der BCT zwischen Akteuren eines Wertschöpfungs-systems mitunter verloren geht. Nach der Flaschenhals-Problematik können entsprechende Handelsakteure mit ihrer bestehenden Marktmacht Zulieferer zur Teilnahme an ihren Blockchain-Systemen auffordern, um ins System liefern zu dürfen. Auf diese Weise kann der LEH einen neuen Transparenzgrad über Zulieferer erlangen und seine Verhandlungsposition entsprechend optimieren.

Aus den analysierten Use Cases ist ein Fokus auf Handelsmarkenprodukte ersichtlich. Daraus lässt sich die Hypothese ableiten, dass eine transparente und sichere Abbildung über alle Prozessstufen von Handelsmarkenprodukten hinweg auf der einen Seite die Verhandlungsmacht des LEH ggü. Markenartikelherstellern verbessern kann und auf der anderen Seite, das Verbrauchervertrauen in eben solche Handelsmarken steigern kann. Aus Sicht der Markenhersteller liegt hierin eine Gefahr des Markenwertverlustes im Vergleich zu Handelsmarken. Der LEH wiederum kann seine Eigenmarken besser schützen und das Risiko von Imageschäden reduzieren. Damit generiert er ein Differenzierungsvorteil ggü. Herstellermarken.

Während der LEH für die Glaubwürdigkeit von Produktaussagen derzeit in erster Linie Produkt- und Qualitätssiegel verwendet, die auf Basis von Auditierungsprozessen unabhängiger Dritter aufgedruckt werden, kann ein vom LEH initiiertes Blockchain-System die

Logik der bisherigen Datenspeicherung solcher Auditierungs- und Zertifizierungsinformationen verändern. Liegen solche Daten der Zulieferer, die sich nach einem gewissen Standard zertifizieren lassen, heute noch auf den zentralen Servern von Zertifizierungs-/Auditierungsgesellschaften, könnte eine dezentrale Blockchain-Lösung die verteilte Speicherung solcher Daten legitimieren. Hierin liegt Chance und Risiko für zuliefernde Akteure zugleich. So könnten Akteure dabei Eigentümer ihrer Datensätze bleiben und diese nur im Falle einer Anfrage an entsprechende Einheiten freigeben. Es könnte aber auch zu einem Informationsgewinn des LEHs hinsichtlich der Zulieferer-Performance führen, sofern dieser den Zugriff auf die Daten im Blockchain-System einfordert oder aber Governance-Regelungen eines „konsortialen“ Blockchain-Systems eingangs durch bestehende Machtverhältnisse entsprechend festgelegt werden.

Der mögliche Transparenzgrad in einem solchen Blockchain-System könnte theoretisch zu einer automatisierten Bepreisung nach bisheriger Performance und einer entsprechenden Rasteroptimierung bei der Lieferantenauswahl je Produkt führen. In einem solchen Gedankenexperiment würde sich der Anreiz, ein entsprechendes Raster zu unterlaufen ggf. mithilfe manipulativer Ansätze für Zulieferer erhöhen. Die Möglichkeiten zur Manipulation könnten sich hierbei lediglich verschieben, aber nicht gänzlich eliminieren lassen (Palka und Wittpahl 2018).

Wenngleich es sich bei den obenstehenden Erläuterungen lediglich um generierte Hypothesen aus den Ergebnissen der vorangegangenen Kapitel handelt, sind die Entwicklungen und Investitionen des LEH in die Blockchain-Technologie aus Sicht der zuliefernden Akteure weiterhin kritisch zu beobachten und von Fall zu Fall die tatsächliche „Konsortialität“ einer solchen Supply Chain-Lösung zu prüfen.

3.4 H4: Blockchain dient in diversen Projekten eher als Marketinginstrument

Die Blockchain-Technologie verspricht mit ihren Eigenschaften Anwendungspotenzial in unterschiedlichen Problemstellungen. Betrachtet man dabei diverse Ankündigungen zur Technologie-Anwendung in verschiedenen Branchen detaillierter, stellt sich allerdings hin und wieder die Frage, inwieweit es sich bei den dort vorgestellten Lösungen tatsächlich um Blockchain-Technologie handelt?

Per Definition können mittels der DLT Datensätze – verteilt gespeichert und kryptografisch verschlüsselt – vor unbemerkter Manipulation geschützt werden, ohne dass es dabei einer zentralen, vertrauensgebenden Autorität bedarf. Neben dem Schutz vor Manipulation, wird durch die BCT also auch die zentrale, verwaltende Instanz disruptiert, wenngleich die Netzwerknutzer weiterhin die Daten auf ihre Richtigkeit prüfen können (Förster 2019).

Vor diesem Hintergrund, gilt es im Einzelfall zu prüfen, inwieweit angekündigte Lösungen v. a. globaler Player der Branche tatsächlich ohne zentrale Instanz im System auskommen und die

Eigenschaften der Blockchain-Technologie nutzen oder wo es sich um ein aktuell nützliches Marketinginstrument handelt. Gerade die Anwendung von Blockchain im SCM oder dem Lebensmittelsektor lässt derzeit Assoziationen wie Transparenz, schnelle Rückverfolgbarkeit, damit höhere Lebensmittelsicherheit und Vertrauenswürdigkeit vermuten. Repräsentative Studien zu dieser Hypothese konnten zu diesem Zeitpunkt nicht ermittelt werden. Dennoch haben verschiedene Gespräche mit Akteuren der Lebensmittelindustrie unter diesem Aspekt die obenstehende Hypothese 4 bestärkt. So kann die Nutzung einer Blockchain-Lösung und Möglichkeit der transparenteren Lieferkettendarstellung ggü. dem Verbraucher im Rahmen des derzeitigen Hypes um die Technologie aus Marketingsicht dienlich sein. Umsatzzahlen des „Blockchain-Geflügels“ von Carrefour wenige Monate nach dem Produktlaunch sind ein Hinweis auf diesen Ansatz (vgl. BTC-ECHO vom 04. Juni 2019). Darüber hinaus können Unternehmen, die sich mit der jungen Technologie in konkreten Use Cases auseinandersetzen, medial als innovative Player ihrer Branche wahrgenommen werden und auf diese Weise ebenfalls ihre Markenwahrnehmung unter Umständen verbessern. Selbst wenn solche Lösungen langfristig keinen Mehrwert in den Prozessstrukturen bringen könnten, so kann es aus marketing-relevanter Sichtweise während des Technologie-Hypes kurzfristig trotzdem interessant sein.

3.5 H5: Eigenschaften der Blockchain kann Unternehmen / Branchen vor Reputationsschäden besser schützen

Während Auditdaten und Zertifizierungsinformationen von Unternehmen heute zentral bei unabhängigen Dritten gespeichert werden, würde eine sog. Audit-Blockchain die entsprechenden Prüfprozesse mithilfe von Timestamps transparent protokollieren. Vertrauliche Unternehmensdaten können dabei durch die Verwendung entsprechender Schlüssel maskiert werden und nur demjenigen zugänglich gemacht werden, der über den entsprechenden Schlüssel verfügt. Für alle anderen Nutzer im System, die den Schlüssel nicht besitzen, bleiben die Daten geheim. Im Falle eines Skandals könnten Informationen auch nachträglich für entsprechende Instanzen freigeschaltet werden, ohne dass sich Prüfinstanzen, zertifizierte Unternehmen oder andere Stakeholder dem Verdacht nachträglicher Manipulation von Daten unterziehen müssten. Korrektes, dokumentiertes Verhalten in der Vergangenheit wäre in einer Blockchain-Lösung also eindeutig nachweisbar.

Anwendungsfälle aus der Logistik zeigen, dass die Ausweitung einer solchen Audit-Blockchain auch auf die Verfolgung von Produkten entlang ihrer Wertschöpfungskette möglich ist. Auf diese Weise bietet die Blockchain-Technologie für Akteure innerhalb solcher Lieferketten Schutz vor unberechtigten Reputationsschäden, selbst wenn sie in einer **vertrauenslosen** Supply Chain agieren. So lässt sich das eigene, korrekte Verhalten mit einem Produkt auf seinem Weg von der Urproduktion bis zum Verbraucher in der Blockchain dokumentieren. Mit einer individuellen Produkt-ID erhält das jeweilige Gut eine Identität in der Blockchain. Mithilfe

von Timestamps kann schließlich dokumentiert werden, wer, wann und wo für das entsprechende Produkt verantwortlich war und worin die Wertschöpfung lag, indem die betroffenen Akteure das Produkt digital in der Blockchain signieren.

Gerade durch Sensordaten und die Kommunikation zwischen verschiedenen Maschinen / Sensoren (IoT) lassen sich mithilfe von IOTA – einer fortgeschrittenen Generation der BCT – manipulationssicher speichern. Diese sichere Datenaufzeichnung über Sensoren ist v. a. dann hilfreich, wenn internationale Lieferketten kontrolliert werden müssen, in denen Länder mit fehlender oder korruptionsgefährdeter zentraler Kontrollinstanz involviert sind. Betrug ist dabei nach wie vor möglich. Die lückenlose Dokumentation des Produktverlaufes und die Gefahr des Reputationsverlustes im System bei Produkten mangelnder Qualität bestrafen Betrugsversuche jedoch. So erlaubt die Aufzeichnung von Auditergebnissen, Monitoring- und Labordaten sowie Kundenfeedback sämtlicher bisher geleisteter Lieferungen eines Akteurs, den Aufbau eines vertrauenslosen Reputationswertes. So können selbst einander gänzlich unbekannte Unternehmen, mit berechenbarem Risiko neue Lieferbeziehungen auf Basis bisheriger Performance im System eingehen. Akteure, die regelmäßig gegen Vorgaben verstoßen, mit Betrugsversuchen ermittelt werden oder kontinuierlich schlechte Reputationswerte haben, könnten mit einem Systemausschluss bestraft werden, wodurch wiederum der Reputationswert des gesamten Liefersystems geschützt werden würde. Auf diese Weise kann neben einem neuen Grad an Vertrauenswürdigkeit zwischen den Teilnehmern auch die des Systems in Gänze gegenüber Verbrauchern steigen.

4 Hypothesen zur Relevanz von Blockchain für QS als Standardgeber

Im folgenden Abschnitt werden Hypothesen über die Bedeutung der Blockchain-Technologie für die QS Qualität und Sicherheit GmbH als Standardgeber erläutert. Die Ableitung dieser Hypothesen basiert auf der umfangreichen Sekundärdatenanalyse, deren Ergebnisse in den vorangegangenen Abschnitten bereits erläutert wurden. Eine wissenschaftliche Hypothesenüberprüfung in Form von qualitativer Primärdatenerhebung und -auswertung wird hier nicht vorgenommen.

4.1 H1: Zentrale, unabhängige Kontrollinstanzen wird es auch in einer „Blockchain-Lieferkette“ bedürfen

Blockchain verspricht, den gesamten Weg eines jeden einzelnen Produktes mittels Produkt-ID und Zeitstempel durch die beteiligten Akteure der Lieferkette dokumentieren zu können und neben Orten, Zeitpunkten, Verantwortlichkeiten sowie einzelnen Prozessschritten sämtliche Zusatzinformationen zu einem Produkt unverfälschbar und transparent abzubilden. Dennoch braucht es eine Kontrolle an der Schnittstelle von physischer Welt zur digitalen Welt. Wenngleich Betrugsfälle leichter ihrem Ursprungsherd zugeordnet werden können, müssen Prozesse bei Produzenten und Verarbeitern vor Ort weiterhin auditiert werden. Ebenso gilt es

weiterhin Standards zu definieren, die möglichst unabhängig vom Interesse einzelner Stakeholder sind. Es braucht also weiterhin Systemarchitekten. Technisch gesehen braucht es hierzu aber keine zentrale unabhängige Instanz mehr. Ein starker Player der Lieferkette könnte die Funktion der technischen Netzwerk-Koordination für die anderen Akteure ebenfalls erfüllen. So kann Blockchain mit ihren Potenzialen bestehende Systemen durchaus weiter optimieren und Effizienz gegenüber aktuellen Dokumentations- und Kontrollprozessen schaffen. Aber eine unabhängige Kontrollinstanz in der physischen Welt wird es auch in einem solchen System benötigen. Jedoch würden sich bestimmte bisherige Aufgaben im Auditierungs-/ Zertifizierungprozess verändern. Es ginge weniger darum, die Sache zu kontrollieren, sondern stärker um eine Kontrolle des Systems. Neben der Abwicklung von Auditierung und Zertifizierung bräuchte es zudem eine Instanz, die Governance-Strukturen für eine Blockchain-Lösung definiert. Zudem müssten Aufbau, Betrieb und technischer Support einer solchen Lösung für die Teilnehmer sichergestellt sein. QS als Standardgeber über die Wertschöpfungsstufen hinweg, bringt bereits heute verschiedene Akteure mit Interessenskonflikten an einen Tisch. Das Pilotprojekt der GS1 Germany GmbH hat in der Analyse bspw. gezeigt, dass es genau eine solche Instanz für den Aufbau einer Blockchain-Lösung mit diversen Akteuren der Branche bedarf. Ohne eine zentrale Instanz, der unterschiedliche Stakeholder vertrauen, wird es erst gar nicht zu einer tatsächlich konsortialen Lösung kommen. Möglicherweise läge in einer solchen Lösung damit eine höhere Akzeptanz der Teilnehmer, als in einer Blockchain-Variante, die primär von einem großen Player der Kette (z. B. LEH) initiiert wurde. Dies hängt letztlich von der Marktmacht ab. Eine ähnliche Kritik wird bspw. gegen das vermeintliche Blockchain-Konsortium von IBM und Maersk gehegt. Wenngleich hierbei die gesamte globale Containerfrachtschifffahrt abgewickelt werden könnte, sträuben sich Reedereien und Spediteure bisher davor, dem Konsortium beizutreten, da die Projektkontrolle bisher zu 50 % bei Maersk und zu 50 % bei IBM liegt. Im GS1-Projekt hingegen hat das Ergebnis gezeigt, dass es für die Problemstellung eigentlich keine Blockchain gebraucht hätte, aber erst so und durch die Koordination von GS1 Germany Unternehmen eine Bereitschaft gezeigt haben, Daten transparent zu machen um Effizienz im Prozess zu steigern. Essentiell ist dabei jedoch: Bisher wurde durch die zentrale Speicherung auch die Glaubwürdigkeit in Bezug auf etwaige Manipulationsverdachte seitens der Lieferkettenteilnehmer erhöht. Denn eine nachträgliche Veränderung von Daten auf einem zentralen Speicher wäre, wenn überhaupt, nur zusammen mit einer zentralen Instanz möglich gewesen. Durch die BCT ist der Aspekt ‚Manipulationssicherheit‘ durch zentrale Speicherung von Daten bei unabhängigen Dritten für ein funktionsfähiges System nicht mehr ausschlaggebend.

4.2 H2: Blockchain könnte zu einem Paradigmenwechsel hinsichtlich des Eigentums an Daten im QS-System führen

Die Logik verteilter Systeme bringt die Möglichkeit mit, dass sämtliche Daten, die ein Netzwerkteilnehmer im System abspeichert, tatsächlich in seinem Besitz bleiben können. Sie müssen nicht auf dem zentralen Server eines Dienstleisters oder in einer verteilten Cloud-Lösung, die aber auch von einem Dienstleister betrieben werden muss, abgespeichert werden. Gleichzeitig kann aber sichergestellt werden, dass der Besitzer eines Datensatzes seine Daten im Nachhinein nicht mehr manipuliert hat, ohne dass es im System aufgefallen wäre. Möchte ein Abnehmer nun Informationen über Monitoringdaten, Auditergebnisse, zusätzliche Leistungen des Lieferanten etc. erhalten, sendet der Lieferant mittels Signatur einen Zugang zu seinen Daten (entweder in Gänze oder dezidiert) an den potenziellen Abnehmer.

Die Umsetzung einer Blockchain-Lösung unter diesem Aspekt müsste für Systemteilnehmer vergleichsweise attraktiv sein. Die Implementierung scheint hier aber herausfordernd zu sein, da Standards hinsichtlich der Dokumentation, Freigaberechte und -pflichten von Systemteilnehmern und dem Umgang mit Zugriffsrechten im Krisenfall eindeutig definiert werden müssten. Es empfiehlt sich daher abzuwägen, inwieweit die heute etablierte, zentrale Speicherung und Verwaltung von Daten durch den jeweiligen Standardgeber von Systemteilnehmern als problematisch eingeschätzt wird und ob darin eine heute ungelöste Herausforderung liegt, die mit einer solchen Blockchain-Variante sinnvoll gelöst werden könnte. Denn auch unter der oben genannten Hypothese gilt, es sollte zuerst ein Problem definiert werden und dann geprüft werden, ob Blockchain eine Lösung darstellen kann und nicht andersherum. Da QS Vertrauenswürdigkeit genießt, ist es möglicherweise nicht für Teilnehmer dieses Systems relevant. Dort, wo Lieferkettenteilnehmer aber einen solchen vertrauenswürdigen Standardgeber nicht vorfinden, kann eine Eigenlösung von dominierenden Lieferkettenteilnehmern naheliegen.

4.3 H3: Blockchain-Technologie als Katalysator für IoT und Big Data könnte künftig die Art und Weise von Audits verändern

Diverse Use Cases und wissenschaftliche Literatur haben gezeigt, dass Blockchain in Kombination mit IoT-Anwendungen zu Effizienzzuwachs führt und Vertrauenswürdigkeit durch automatisierte Aufzeichnungen von Zuständen innerhalb der Lieferkette steigern kann. Um Auffälligkeiten durch Sensoraufzeichnungen oder IoT-Aktivitäten in Lieferketten zu erkennen und daraus Fehlerquellen automatisiert ableiten zu können, reicht es nicht aus, einzelne Betriebe mit IoT-Lösungen auszustatten und gesondert zu betrachten. Erst mit der ganzheitlichen Aufzeichnung sämtlicher Prozesse im System kann dabei ein Mehrwert generiert werden. BCT in seiner 3. Generation (z. B. IOTA) liefert dabei Möglichkeiten, bisherigen Herausforderungen von IoT und Big Data in puncto Privatsphäre bzw. Datenschutz und Manipulationssicherheit zu begegnen.

So könnte Blockchain eine Anwendung von IoT in Fertigungs- und Logistikprozessen rechtfertigen, um beispielsweise Wartungsintervalle, Temperaturregulierung, Fahrzeiten etc. zu prüfen. Mithilfe von Smart Contracts ließen sich solche Prozesse dabei weitestgehend automatisieren. Die Dokumentation solcher Daten über das gesamte QS-System hinweg könnten mit der Anwendung von Big Data helfen, um Anomalien automatisiert zu identifizieren und Fehlerquellen für solche Abweichungen sowie Prognose über künftige Datenwerte zu ermitteln. Damit ließe sich langfristig eine Verschiebung des zu prüfenden Zustandes in einem Audit realisieren. Anstelle der Kontrolle vergangener Aufzeichnungen liefern IoT-Systeme Informationen in Echt-Zeit in das System. Entsprechende Big Data-Lösungen könnten daraus wiederum künftige Zustände ableiten und Auditempfehlungen ermitteln.

Die Hypothese zeigt, dass ein Blick auf die Entwicklung weiterer Technologien, die im Rahmen der Digitalisierung für Aufsehen sorgen, mehr als zu empfehlen ist, da sich oftmals erst durch die Kombination unterschiedlicher Technologien tatsächliche Mehrwerte generieren lassen.

4.4 H4: Derzeitige Blockchain-Entwicklungen im Handel könnten u. U. zu einer stärkeren Verhandlungsmacht des LEHs ggü. Zulieferern und auch dem QS-System führen

Die Analyse bisheriger Blockchain-Projekte im Lebensmittelsektor zeigt, dass in erster Linie vom Handel ein Hype um die Technologie in der Branche ausgeht. Meistens mit dem Ziel, Lebensmittelsicherheit, Transparenz und Schutz vor Lebensmittelbetrug zu optimieren. Bei genauerer Betrachtung von Projekten, die bspw. Walmart oder Carrefour initiiert hat, fällt auf, dass dabei der eigentliche Gedanke von Blockchain (Demokratisierung und Disintermediation) in weiten Teilen hinfällig wird. So liegt die Definition der inhaltlichen Standards bei den entsprechenden LEH-Playern und die technische Umsetzung der Blockchain-Lösung beim IT-Anbieter IBM mit seiner Lösung „IBM Food Trust“. Gerade die Walmart-Projekte zeigen, dass sich die Verhandlungspositionen dabei nicht von zentralen Lieferantensystemen unterscheiden und auch mit IBM Food Trust eine deutliche Verhandlungsmacht vom LEH ausgeht. Blockchain erlaubt hier im Gegenteil eher einen Transparenz-Gewinn für den LEH in die vorgelagerten Wertschöpfungsstufen auf der einen Seite und einen Markenwert-relevanten Zugewinn gegenüber Verbrauchern auf der anderen Seite. So lässt sich eine Herkunftsdokumentation auf der Blockchain gegenüber dem Konsumenten als transparent, sicher und vertrauenswürdig vermarkten.

Für den LEH kann eine Blockchain-Lösung im Lieferantenmanagement zudem attraktiv sein, da Prüfprozesse entlang der Lieferkette z. T. automatisiert werden können und eben in Krisenfällen eine sehr schnelle Identifikation von Ursachenquellen realisierbar ist. Inwieweit der LEH für diese Prozesse im Rahmen einer Blockchain-Lösung noch von einem dritten, unabhängigen Standardgeber / Zertifizierer abhängig ist, bleibt an dieser Stelle offen. Es ist aber zu vermuten, dass der Bedarf einer solchen Rolle für den LEH-Player eher abnehmen

würde. Aus diesem Grund empfiehlt sich für die QS als Standardgeber und Mittler zwischen den unterschiedlichen Stakeholdern in einer Lieferkette, ein besonderes Augenmerk auf die Entwicklungen im LEH zu haben, da von dort aus am ehesten disruptive Entwicklungen ausgehen könnten. Denn dieser hat ein großes Interesse an den wesentlichen Vorteilen einer sehr schnellen Rückverfolgbarkeit. Dies dürfte auch von Seiten des Gesetzgebers und staatlichen Kontrollinstanzen als wesentlicher Vorteil ggü. jetzigen Systemen gesehen werden. Da die Dauer der Aufklärung in Krisenfällen hohen Druck auslöst und auch mediale Angriffspunkte darstellt.

5 Kritische Würdigung der Methoden und Ergebnisse, Fazit und Ausblick

Im nachfolgenden Kapitel werden die kritische Betrachtung der verwendeten Methoden sowie die Ergebnisse des Projektes synoptisch zusammengefasst. Ausgehend von den vorangegangenen Hypothesen erfolgt eine abschließende Handlungsempfehlung für den weiteren Umgang mit der Blockchain-Technologie.

5.1 Kritische Würdigung der Methoden und Ergebnisse

Im Rahmen einer mehrstufigen Sekundärdatenanalyse konnten im ersten Schritt die Funktionsweisen der Blockchain-Technologie erläutert werden. Der Fokus wurde dabei neben allgemeiner Literatur aus dem Feld der Distributed Ledger Technologie, ergänzend auf Literatur des Supply Chain Managements und der Logistik gelegt, worin sich mit den Funktionsweisen der Blockchain-Technologie auseinandersetzt wird. Für die technische Bewertung, unterteilt in Herausforderungen und Risiken sowie Chancen und Potenziale von BCT sowie für die Betrachtung technischer Weiterentwicklungen wurde ebenfalls Fachliteratur aus den o. g. Feldern verwendet. Die Berücksichtigung unterschiedlicher Autoren, hilft bei den teilweise unterschiedlichen Sichtweisen hinsichtlich der Technologie-Bewertung eine möglichst objektive Einordnung geben zu können.

Zur Beantwortung der Fragestellung „Welche Entwicklungen und Projekte hinsichtlich der Anwendung von DLT sind im Agri-Food-Sektor zu beobachten?“, wurde im Folgeschritt ebenfalls auf Basis einer Sekundärdatenanalyse bisher publizierte Pilotprojekte, Use Cases sowie marktreife Blockchain-Produkte der Branche betrachtet und tabellarisch im Anhang zusammengeführt. Neben Projektinhalten wurden dabei Initiatoren und involvierte Player sowie Zeitpunkt und Ursprungsort ermittelt. Auf Basis der über 80 analysierten Projekte konnte im Anschluss eine inhaltliche Clusterung nach den Anwendungsschwerpunkten von Blockchain für die Branche vorgenommen werden. Dabei haben sich drei Cluster ergeben: Supply Chain Management, Auditierung und Zertifizierung sowie IoT. Die daraus abgeleitete Hypothesengenerierung erfolgte neben den Erkenntnissen der Sekundärdatenanalyse auf diversen Feedbackgesprächen mit Akteuren der Lebensmittelbranche. Es verbleibt dabei aber ebenfalls bei einer hypothetischen Einschätzung zu der Relevanz von Blockchain für die Branche bzw. das QS-System. Eine Überprüfung der durch die Autoren ermittelten Hypothesen unter Verwendung von Methoden der qualitativen Primärdatenanalyse wurde im Rahmen dieses Projektberichtes noch nicht vorgenommen. Dies sollte Gegenstand weiterer Folgearbeiten sein.

Zur kritischen Diskussion der Ergebnisse wird im Folgenden eine synoptische Zusammenfassung über die Bewertung der Blockchain-Technologie gegeben. Im nachfolgenden Kapitel 5.2 erfolgt dann ein abschließendes Fazit sowie denkbare

Handlungsempfehlungen hinsichtlich der Relevanz von Blockchain für die Agri-Food-Branche und schwerpunktmäßig für das QS-System.

Tab. 8: Stärken, Schwächen, Chancen und Risiken der Blockchain-Technologie

<p>Stärken</p> <ul style="list-style-type: none"> ✓ Vertrauensgebende, zentrale Instanz bzw. Vertrauen zw. Akteuren braucht es nicht unbedingt ✓ Daten sind vor Manipulation und Löschung geschützt ✓ Hohe Datenintegrität und Schutz vor Hackerangriffen von außen ✓ Single Source of Truth löst Problem von Informationsasymmetrien ✓ Kein Single Point of Failure und damit hohe Redundanz ✓ Möglichkeit differenzierter Zugangsberechtigungen ✓ Individuelle Programmierung möglich 	<p>Schwächen</p> <ul style="list-style-type: none"> - Skalierbarkeit und Speicherkapazität durch kontinuierliches Wachstum einer Blockchain im Zeitverlauf ihrer Nutzung noch nicht in Gänze gelöst - Informationen sind irreversibel. Einmal gespeichertes oder fehlerhafte Smart Contracts sind quasi nicht rückgängig zu machen
<p>Chancen</p> <ul style="list-style-type: none"> ✓ Breites Feld an möglichen Anwendungen (Finanz, IoT, Versicherungen, Shared Economy, Supply Chain, Governance, etc.) ✓ Kompatibilität und damit ggf. Katalysator für Anwendungen aus den Bereichen IoT, Big Data, Cloud-Services usw. ✓ Steigerung der Transparenz von Waren-, Geld- und Informationsströmen ✓ Massive Optimierung der Rückverfolgbarkeitsgeschwindigkeit (wenige Sekunden) schafft neues Maß an Sicherheit im Krisenfall ✓ Hoher Grad an Cyber Security ✓ Ermöglicht neue Geschäftsmodelle ✓ Bisher potentialreicher Lösungsansatz für SCM und Lebensmittelwirtschaft, Pharma, Internationaler Handel etc. 	<p>Risiken</p> <ul style="list-style-type: none"> - Fehlerhafte Programmierung stellt massives Sicherheitsrisiko dar, wie Bsp. aus der Vergangenheit belegen - Sicherheit des Systems ist erst bei Erreichen einer kritischen Anzahl Teilnehmer gegeben - Bisher sind rechtliche und regulatorische Fragen noch nicht klar gelöst - Paradigmenwechsel ganzer Branchen nötig (Transparenz statt „Silodenken“) - Kosten noch unklar

5.2 Fazit und Handlungsempfehlungen

Verschiedene Use Cases haben gezeigt, dass es nicht immer einer BCT für die Lösung des jeweils anvisierten Problems bedarf. Zum Teil erweckt es eher den Eindruck als hätte zuerst die Blockchain-Lösung und der Wunsch einer solchen bestanden, bevor ein Problem zur Anwendung definiert wurde. Diverse Autoren, die sich mit der Anwendung von Blockchain-

Technologie befassen, empfehlen dabei ausdrücklich die Definition eines konkreten Problems im ersten Schritt. Erst danach gilt es eine Lösung zu entwickeln und hierbei ggf. auf einen dezentralen Ansatz mittels BCT zurückzugreifen. Für diesen ersten Schritt gibt Hosp (2018) einen Fragenkatalog zur konkreten Problemidentifikation und -definition vor, aus dem sich folgende Fragen für Kunden und/oder Mitarbeiter der eigenen Organisation empfehlen:

- Was stört Sie in Ihrem Berufsalltag?
- Wer könnte durch diesen Punkt in seinem Berufsalltag ebenfalls behindert werden?
- Für welche Dienstleistungen und Services sind im Unternehmen Ihrer Meinung nach zu teuer bzw. ließen sich kostengünstiger abbilden?
- Welche Prozesse sind aufgrund von Vertrauensmangel durch Ineffizienzen geprägt?
- In welchen Prozessen sehen Ihre Kunden ein Vertrauensproblem?

Nach der Identifikation bestehender Probleme bzw. Verbesserungspotenziale in der Organisation stellt sich die entscheidende Frage: Zentrale Datenbank oder Blockchain? – wie aus vorangegangenen Abschnitten bereits hervorgegangen ist, bestehen heute z. T. Blockchain-Lösungen, die im Grunde nur wegen des Hypes um die Technologie auf eben dieser basieren. Die Auseinandersetzung mit dieser Fragestellung sollte daher umso kritischer erfolgen. Diverse Beratungsgesellschaften und Anbieter von BCT-Lösungen haben hierzu Entscheidungsbäume entwickelt, die sich untereinander häufig kaum unterscheiden. Die finale Entscheidung sollte nicht nur auf der Bearbeitung eines solchen Diagramms erfolgen, sie kann aber wesentlich dadurch unterstützt werden und veranschaulicht nochmal, dass es nicht immer einer Blockchain bedarf, sondern es auf den Use Case ankommt, ob diese technische Lösung vorteilig ist. Die nachfolgende Abbildung zeigt einen solchen Entscheidungsbaum, der aus bestehenden Entscheidungsmodellen nach (Peck 2017; Kückelhaus et al. 2018; Meunier 2018) im Rahmen des Projektes entwickelt wurde. Weitere Entscheidungsbäume bspw. von McKinsey, IBM oder Accenture können ergänzend dazu in den Prozess einbezogen werden.

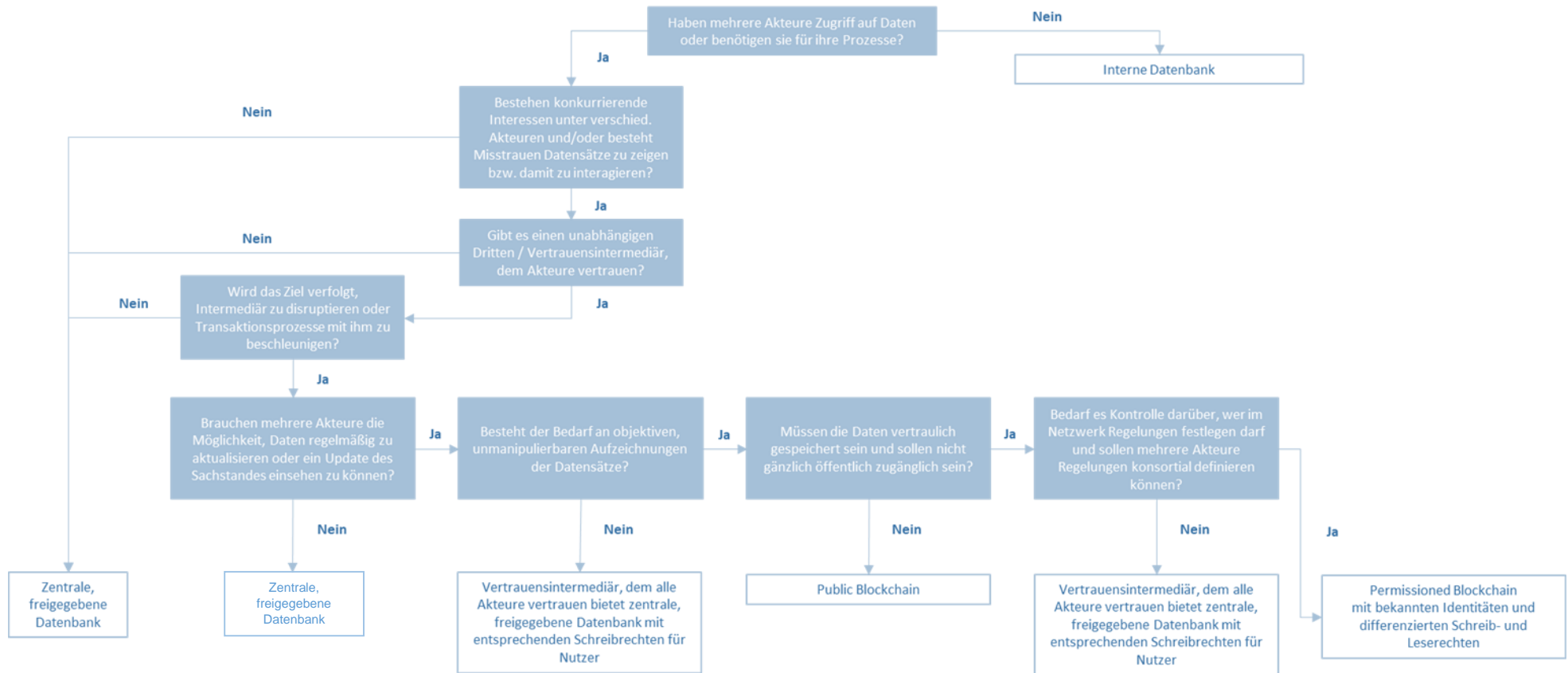


Abb. 13: Entscheidungsbaum für Verwendung von Blockchain (i. A. an Peck 2017; Kückelhaus et al. 2018; Meunier 2018)

Sollte sich für eine Problemstellung die Verwendung einer dezentralen Lösung empfehlen, sollte sich im ersten Schritt die Nutzung einer bereits bestehenden Blockchain bedient werden. Zumindest für den Proof-of-Concept lassen sich die allermeisten Use Cases in bereits vorhandenen Blockchains deutlich kostengünstiger realisieren, anstatt eine komplett neue Lösung aufzusetzen.

Für einen ersten Proof-of-Concept von Blockchain für das QS-System empfiehlt es sich außerdem folgende Punkte zu berücksichtigen (Hosp 2018; Drescher 2017):

- Sämtliche Akteure (Systemteilnehmer, Auditoren, Zert.Stellen etc.) einer ausgewählten Lieferkette sollten bereits im Konzeptionierungsprozess involviert sein, um eine kollaborative Lösung zu erarbeiten und keine Wertschöpfungsstufe „abzuhängen“.
- Vom Einfachen zum Komplexen: Für die ersten Schritte mit der neuen Technologie, kann eine Lieferkette mit hoher Integration sinnvoll sein, da hier der Paradigmenwechsel von Informationssilos zu „verteilten“ Daten weniger gravierend ausfällt. Nach erfolgreichem Abschluss der Testphase können erste Learnings dann auf komplexere Systeme angewendet werden.
- Untersuchte Projekte zeigen, dass sich ein limitierter Zeitrahmen für den eigentlichen PoC empfiehlt, um Mehraufwand für die beteiligten Player überschaubar zu halten. Die Analyse zeigt, dass ein Zeitfenster von 10 – 14 Tagen, in denen das Blockchain-System tatsächlich arbeitet ausreichend sein kann.
- Für die Konzeptionierung und Problemidentifizierung empfiehlt sich bereits die Hinzuziehung von technischen Blockchain-Experten, die Machbarkeit sowie Sinnhaftigkeit technisch beurteilen können.

Als abschließende Einschätzung, basierend auf den für dieses Projekt berücksichtigten Erkenntnissen, lässt sich Folgendes hinsichtlich der Relevanz von Blockchain für die Agrar- und Lebensmittelbranche zusammenfassen. Es wird vermutlich auch in Zukunft weiterhin zentrale Lösungen und Services geben, um die heutige Performance in Wertschöpfungsketten realisieren zu können, aber man muss sie zukünftig nicht immer zwangsläufig nutzen. So werden etablierte, zentral-orientierte Organisationen in Zukunft an verschiedenen Stellen von distribuierten Systemen herausgefordert werden. Heutige Use Cases, die sich bereits im Roll-Out befinden oder diesen ankündigen, weisen darauf hin. Für erfahrene zentrale Organisationen empfiehlt sich daher, für ihre Kunden das Beste aus zentralen und verteilten IT-Lösungsansätzen zu nutzen. Erkennen Unternehmen die Möglichkeiten der Blockchain-Innovationen bzw. der verteilten Speicherung und erstellen einen nutzerorientierten Mix aus beiden Welten, können sie mit ihrem Erfahrungsschatz und der Innovations-Offenheit ggü. reinen dezentralen Organisationen bestehen. Ein Ignorieren oder Ablehnen der Technologie kann für etablierte Akteure mittel- bis langfristig existentielle Gefahren bergen.

Anhang

No.	Company Partner	Typ	Beschreibung	Blockchain-Technologie	Region	Startzeit	Quelle
1	Full Profile is the company behind AgriDigital	Start-Up	<ul style="list-style-type: none"> Real-time transactions for farmers through smart contracts running on a blockchain Payments can be made immediately following the transfer of asset ownership 	AgriDigital	Australien	2016	Fullprofile.com.au https://www.startupdaily.net/2016/06/sydney-agritech-startup-full-profile/
2	Beefledger	Start-Up	<ul style="list-style-type: none"> Australian beef traceability initiative focusing food fraud in China and the decrease of customers' trust in the authenticity of imported high-quality beef from Australia 		Australien	2018	https://bitcoinputrize.com/wheres-the-beef-australian-insurer-joins-beefledgers-blockchain-based-supply-chain-trial.html
3	TE-Food GmbH	Start-Up	<ul style="list-style-type: none"> Government and TE-Food started pilot for supply chain traceability of pig trade 2017 extended to chicken, eggs (> 6.000 companies as user) Currently, TE-Food is world largest whole supply chain tracking network 2018, expanded to track cattle, fish, seafood, fruits, vegetables Customer: Governments, private companies, certification bodies Provenance and trust into food quality as main benefit for customer 1D/2D and RFID connected with mobile and web based software for traceability etc. 	FoodChain based on Rinkeby Network. Rinkeby is an Ethereum testnet and uses a Proof of Authority (PoA) consensus algorithm.	Germany	2015	https://co.lefoodint.com/ https://steemit.com/cryptocurrency/@te-food/te-food-the-world-s-largest-farm-to-table-food-ecosystem-is-moving-to-blockchain-and-tokenization
4	Barclays	Commodity	<ul style="list-style-type: none"> Letter of Credit guaranteeing a \$100k dairy product export – Commodity Financing Based on the BCT platform of Wave Time optimization: normally needed time of 7-10 days to 4 hours for the complete process 		Irland	2016	https://www.reuters.com/article/us-banks-barclays-blockchain/barclays-says-conducts-first-blockchain-based-trade-finance-deal-idUSKCN11D23B
5	AgriDigital-Platform of FullProfile + Fletcher Intl. Exports	Commodity	<ul style="list-style-type: none"> Sale of 23 metric tonnes of wheat from an independent wheat grower to Fletcher International Exports Cloud-based commodity mgmt. Solution to connect farmers, buyers, site operators, financiers and allowing them to contract, deliver and make payments in real-time (using smart contracts, IoT, Sensors etc.) Commodity Sales started with grain they are expanding in rice and cotton industries Agri digital's business model: SaaS platform to simplify commodity management, supply chain finance and optimize traceability in agribusinesses with Smart Contracts. Further pilots of AgriDigital: CBH Group (2017), Rabobank (2017) 	Private Blockchain based on Ethereum	Australien	2016	https://www.agridigital.io/reports/case-study-fletcher-international-exports https://www.afr.com/technology/wheat-farmers-trial-blockchain-to-sell-grain-and-find-it-is-fast-and-reliable-20161206-g57lx
6	Walmart, Tsinghua University, IBM	Retail	<ul style="list-style-type: none"> Track & Trace of Walmart's Pork Supply Chain in China and its production in the US Targeting to boost efficiency and enhance the food safety standards Dec. 2017: Collaboration with JD.com as Blockchain Food Safety Alliance for food tracking and enhancing food security in China Currently, Walmart has filed for about 50 blockchain patents Walmart is able to track 25 products (Strawberries, yogurt, chicken from five suppliers, since Sept. 2018 all lettuce and spinach suppliers of Walmart have to log their shipments on the blockchain. 	Hyperledger Fabric	China, Usa	2016	Coindesk, Nasdaq, Forbes https://www.forbes.com/sites/rogeraliken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#48ed65c7d9c
7	AgriLedger	Start-Up	<ul style="list-style-type: none"> Focus on tracing food origins, getting easier access to financing and secure storing of transaction data in developing countries to help farmers retaining bigger share of their crop value AgriLedger uses a mobile app to deliver smallholders and co-ops a complete framework of trust for buying, selling and sharing Vision of AgriLedger: reducing the lack of transparency, open currently restricted access to price data and tackle corruption 		Großbritannien	2016	http://www.agriledger.io/about/ https://www.startus-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-agricultural-industry/
8	Provenance	Start-Up	<ul style="list-style-type: none"> 6 month pilot to track and trace yellowfin tuna 		Indonesien	2016	https://www.provenance.org/tracking-tuna-on-the-blockchain
9	HARA	Start-Up	<ul style="list-style-type: none"> Start-up combining blockchain and AI for data exchange in the food and agriculture sector since 2015 Focussing on the collection of hard-to-into-data (farmer, land, weather data) in different regions of Indonesia to develop beneficial data-driven decision-making/supporting tools this helps to digitize loan administration and disbursement process of financial institutions 		Indonesien	2018	https://haratoken.io/
10	ARC-net	Start-Up	<ul style="list-style-type: none"> Tackle food fraud by using DNA sampling to verify food sources To assure customers the provenance and authenticity of products the path of a product to the market is documented in a blockchain 		Irland	2017	agfundemews
11	CBH Group + AgriDigital	Commodity	<ul style="list-style-type: none"> Trading Oats to china on a blockchain as a pilot project 	Private Blockchain based on Ethereum	Australien	2017	https://www.ethnews.com/agridigital-partners-with-cbh-to-track-oats-on-the-blockchain
12	Costco Wholesale	Food Processing	<ul style="list-style-type: none"> Part of the IBM-Food-Trust-Pilot in 2017 together with Nestle, Walmart, Tyson Foods, Mc Cormick, Glan State Foods 	IBM	USA	2017	https://www.forbes.com/sites/rogeraliken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/#7128f97d3d36
13	Crunchies, Deloitte	Food Processing	<ul style="list-style-type: none"> Introduction of a blockchain-based traceability platform with a traceability button on ist website, allowing customers to enter the lot code on a packet to find the source of the product and explain why a particular product was sourced from a given country. First tests based on their Strawberry supply chain from three different countries 		USA	2017	https://www2.deloitte.com/insights/us/en/industry/retail-distribution/food-labeling-laws-10-blockchain.html
14	Nestlé	Food Processing	<ul style="list-style-type: none"> more than 10 blockchain pilot projects in 2017-2019 Using IBM Food Trust to track the provenance of food ingredients, including Gerber Baby Food 	IBM Food Trust Blockchain	Europe	2017	https://www.forbes.com/sites/michaeldecastillo/2019/04/16/blockchains-billion-dollar-babys/#2a1d8adc30a5
15	Walmart Costco, Nestle, Dole, Unilever,	Konsortium	<ul style="list-style-type: none"> IBM Food Trust Pilot project: enhance the transparency and quality assurance as well as the knowledge about food origin for consumer. Optimization of network control, time and cost reduction and increased process efficiency as major values for involved companies Major result of the pilot: Tracking mangoes supply chain in 2.2 seconds instead of 20 hours 	Hyperledger	USA, China	2017	https://www.supplychain24.com/article/major_blockchain_collaboration_to_address_food_safety_worldwide https://jbs.scholasticahq.com/article/3712-food-traceability-on-blockchain-walmart-s-pork-and-mango-pilots-with-ibm https://www.supermarketnews.com/food-safety/more-retailers-join-ibm-food-trust-network
16	Foodchain.it	Start-Up	<ul style="list-style-type: none"> Provides Food Traceability based on blockchain platform combined with IoT-sensors 		Italien		https://food-chain.it/public/business/
17	TwigaFood + IBM	Start-Up	<ul style="list-style-type: none"> Micro-loans based blockchain in Africa TwigaFoods is a Kenyan start-up providing an online-logistics-platform for food kiosks 	IBM	Kenia	2018	https://www.ibm.com/blogs/research/2018/04/ibm-twiga-foods/
18	BananaCoin	Start-Up	<ul style="list-style-type: none"> BananaCoin is the world's first blockchain option for participating in the production of organic bananas in Vientiane province, Laos. 		Laos	2016	https://bananacoin.io/
19	FoodTrax	Start-Up	<ul style="list-style-type: none"> Traceable, ethical asian food for the european market under private labels 		Niederlande	2017	https://www.foodtrax.nl/index.html
20	BASF + ARC-net	AgChem	<ul style="list-style-type: none"> Partnership for developing a software-solution to document the ecological footprint in ag AgBalance Livestock is a BASF-developed software for more sustainable animal protein production which is combined with the blockchain-solution of ARC-net 		USA, Irland	2018	https://www.basf.com/global/de/media/news-releases/2018/04/p-18-174.html

No.	Company Partner	Typ	Beschreibung	Blockchain-Technologie	Region	Startzeit	Quelle
21	Bayer Crop Science + BlockApps + ConsenSys	AgChem	• Cooperation started in March 2019, first projects are already running since 2018			2018	https://de.cointelegraph.com/news/bayers-agricultural-division-partners-with-consensys-backed-startup-blockapps
22	AgOS	Start-Up	AgOS brings together information flows across agri-food supply chains to give chain managers, stakeholders and consumers a full, transparent & end-to-end view of the goods flow. - End to End Chain Visibility - Integrated Finance - Trust and Transparency - Creating a digital goods passport		Niederlande	2018	http://agos-tech.com/
23	GS1	Certification	• Pilotprojekt zum Palettentausch zwischen Akteuren in Lieferketten auf Blockchain-Basis • Involvierte Partner: Beiersdorf, Bosch, DB, DHL, dm, Dole Foods, Dr. Oetker, dwf, Kaufland, Lekkerland, MARKANT, MARS, Metro Logistics, Nagel Group, PWC, FIEGE, Gärtnerei Utenburg, hagebau, HENKEL, Riegerink, Ringoplast, SPAR, SAP, T-Systems, Vöslauer, Wernsing Food Family, u.a.		Germany	2018	https://www.gs1-germany.de/fileadmin/gsl/basis_informationen/was_kann_blockchain_wirklich.pdf
24	ABCD-Konsortium	Commodity	• ABCD quartet will use Distributed Ledger Technology (DLT) and Artificial Intelligence (AI) to monitor trade. • focusing a more transparent and cost-effective commodities trade world wide		World Wide	2018	https://blockchainreporter.net/2018/10/27/abcd-bringing-blockchain-to-the-agricultural-sector/
25	BNP Paribas + HSBC Singapor	Commodity	• Change paper-based letters of credit to a secure blockchain solution • 1st fully digitized commodity letter-of-credit transaction in Sept. 2018	Corda, Hyperledger Fabric, Ethereum	France, Singapor	2018	https://www.forbes.com/sites/michaeldecastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8ad30e6
26	Cargill, HSBC, ING	Commodity	• BC-based Soybean trade transported from Argentina to Malaysia		Agrentinen, Malaysia	2018	https://www.businessinsider.de/hsbc-ing-blockchain-trade-finance-cargill-soybeans-2018-53?u=US&R=T
27	Louis Dreyfus	Commodity	• Commodity Trading based on BCT-transaction system as pilot project • Shandong Bohi Industry (Boh), ING, Societe Generale + ABN Amro • According to Bohi as soybean trader, the test involved a shipment of soybeans from the U.S. to China including contract documents as well as the letter of credit in the bct-platform • Reduction of trade processing time for Louis Dreyfus: 80 %		World Wide	2018	CoinDesk, Cointelegraph, Financial Times
28	ARLA	Food Processing	• Testing blockchain-technology in their "Aria Milkchain" in Finland		Finland	2018	https://www.arla.fi/artikkelit/arla-milkchain-the-blockchain-for-more-transparent-milk-production/
29	Barilla + IBM	Food Processing	• Using Blockchain to tackle transparency and traceability in its pesto production cycle • Cultivation, Treatment, harvesting in the field, transportation, storage, quality control to production are tracked in a blockchain • QR-Code for consumers	IBM	Italia	2018	https://bitnewstoday.com/market/blockchain/icom-of-italian-business-opt-for-blockchain/
30	Tyson Foods	Food Processing	• Member of the FoodLogIQ Consortium for Blockchain Technology		USA	2018	https://www.tysonfoods.com/the-feed-blog/blockchain-ing-our-way-stronger-supply-chain
31	FSA	Governance	• Food Supply Chain Transparency for beef • 1st Pilotproject focusing the documentation of food safety standards in a slaughterhouse • Following projects are planned		Großbritannien	2018	https://www.food.gov.uk/news-alerts/news/isa-trials-first-use-of-blockchain
32	South Indian State Kerala	Governance	• Governmental project (initiated by the Development and Innovation Strategic Council K-DISC): Blockchain for an optimized distribution of food supply of dairy products, vegetables and fish • Combining IoT with Blockchain to monitor informations about a product's source, production, quality and distribution • Second blockchain project focusing crop-insurance, ensuring tamper-proof and efficient processing and settlement claims for farmers suffering crop losses.		India	2018	https://www.business-standard.com/article/pti-stories/kerala-govt-to-leverage-blockchain-tech-to-streamline-supply-118061700269_1.html https://de.cointelegraph.com/news/south-indian-state-of-kerala-to-use-blockchain-tech-in-food-supply-distribution
33	FoodLogIQ	Konsortium	• FoodLogIQ as leading SaaS-Provider of traceability, food safety and supply chain transparency solutions initiated a Consortium for traceability of food supply chains based on blockchain • Members: Tyson Foods, Subway, Testo, AgBiome Innovations and others		USA	2018	https://www.foodlogiq.com/solutions/blockchain/
34	Maersk	Logistics	• TransLens as a global BCT-based system to track freight shipping – Track & Trace • Pilot: Shipper, buyer, customs, US Homeland Security were included • Reduction of paperwork as main target of this initiative • 100 Organizations already have signed up to use the platform	IBM Blockchain, Corda	USA	2018	https://www.forbes.com/sites/michaeldecastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8ad30e6 https://www.tradelens.com/ https://www.datacenter-insider.de/tradelens-von-maersk-und-ibm-soll-das-schiffahrtsoekosystem-umkampeln-a-741365/
35	WWF, Viant, MSC	NPO	• Pilot project to stamp out illegal, unreported and unregulated fishing and human rights abuse in the Pacific Islands' tuna industry • Focus on Traceability: track albacore tuna by sensors. Fish are tagged with a sensor when caught, sensor interacts with AIS transmitter to record time and location. Location data confirms that fish were caught in a place where fish stocks are not over-exploited.	Viant (Ethereum)	New Zealand	2018	https://media.consensys.net/watch-how-viant-tracks-sustainable-fish-from-bait-to-plate-with-blockchain-tech-9ff46e443e
36	Oxfam	NPO	• Pilot Project: Organic rice traceability initiative "BlocRice" to empower farmers in their price negotiations and in finding buyers • Supported by the Ministry of Agriculture, Forestry and Fishery, NGO Development and Partnership in Action (DPA) and Sdao Aphiwat Agriculture Co-operative • Three main project targets: cashless payments based upon digital acceptance of delivery, Smart Contracts between supply chain members, Providing customer information of the organic rice		Cambodia	2018	https://www.ledgerinsights.com/oxfam-blockchain-cambodian-rice-farmers/ https://www.oxfamamerica.org/explore/stories/can-blockchain-help-rice-farmers-fight-poverty/
37	Carrefour + IBM	Retail	• Launch of the first BCT-based system for food traceability in Europe • Chicken, Roll-out is planned for eggs, cheese, milk, oranges, tomatoes, ground beef and salmon • BCT „can be used in the food sector so that each and every party along the length of the supply chain (...) can provide traceability information about their particular role and for each batch (dates, places, farm buildings, channels, potential treatments, etc.)“ • QR codes as product labels will help customers to get detailed information about the products journey	IBM	Frankreich, Spanien	2018	http://www.carrefour.com/current-news/food-traceability-carrefour-a-blockchain-pioneer-in-europe-has-joined-the-ibm-food
38	Gustav Gering	Retail	• Seafood Traceability and Trading with seafood on a Ethereum blockchain platform of products that are MSC certified • Information about Capture and Processing: Shipper, Capture time, method and area as proof of a sustainable production • Ajato as Software-provider developed specific smart contracts based on Ethereum. It partners with ConsenSys	Ajato, Bangkok	Schweiz	2018	https://blockchainwelt.de/justav-gering-nutzt-blockchain-zum-handel-mit-msc-thunfisch-produkten/
39	Provenance + The Co-Operation Group	Retail	• Track and Trace of Food Supply Chain for authenticity and sustainability		Großbritannien	2018	https://www.provenance.org/case-studies/co-op

No.	Company Partner	Typ	Beschreibung	Blockchain-Technologie	Region	Startzeit	Quelle
40	REWE Seleggt	Retail	<ul style="list-style-type: none"> Using BCT to track the production of Seleggt-eggs 		Germany, Netherlands	2018	https://www.presseportal.de/pm/52007/4109798
41	Hello Tractors + IBM	Start-Up	<ul style="list-style-type: none"> mobile App-Service for smallholders to rent tractors in Africa Startup partners with John Deere Idea is a blockchain- and AI-based platform for a transparent and trustworthy network between farmers, tractor fleet owners, financial institutions, etc. 	IBM Food Trust	Nigeria	2018	https://www.ibm.com/blogs/research/2018/12/hello-tractor/
42	OriginTrail	Start-Up	<ul style="list-style-type: none"> Startup with traceability initiative in a way to store a "fingerprint" on the blockchain Cost reduction to cents per item Created a Trace Alliance as consortium (Deloitte, H&M Trail, Oregon Tilth, Phy2Trace, ...) 		Slovenia	2017	https://medium.com/origintrail/origintrail-monthly-report-march-2019-583bf4435203
43	Ambrosus	Start-Up	<ul style="list-style-type: none"> High tech sensors, blockchain protocol and smart contracts to build a universally verifiable, community-driven ecosystem to assure food quality, safety and origins of products. Traceability 		Switzerland	2017	ambrosus.com https://finlantern.com/fundforum/wp-content/uploads/2017/11/ambrosus-lugano.pdf
44	OwlTing	Start-Up	<ul style="list-style-type: none"> Developed the OwlChain as direct sales platform for food, travel, ... 		Taiwan	2010	
45	SkuChain	Start-Up	<ul style="list-style-type: none"> Developed in the Bitcoin network to provide security and visibility for global supply chains A system for next generation identifiers in form of barcodes and RFID tags to digitally secure the transfer of goods across the entire global economy SkuChain provides cryptographic proof of each SKU's origin and supply chain that can be verified all the way to the point of consumption 		USA	2014	http://www.skuchain.com/
46	Ripe Technology	Start-Up	<ul style="list-style-type: none"> Focus on increasing transparency of fresh produce food supply chains by answering the questions: What is our food? Where has it been? What happened to it? Which certifications has a specific product? Ripe.io creates with new analytics, automation and IoT and a blockchain protocol a new way to visualize a product's journey First pilot dealt with the Tomatoe Supply Chain: sensors for light, temperature, humidity etc. 	ripe.io-Plattform	USA	2017	ripe.io
47	Aniheuser-Busch InBev (AB InBev)	Food Processing	<ul style="list-style-type: none"> Pilot Project in San Francisco Bay Area: Consumers upload driver's licences information to a blockchain to buy their beer at a vending machine by scanning their phone Partnership with BanQu in Africa (faster growing market for beer): using blockchain to provide pricing information and payments to farmers lacking bank accounts. Benefit: Access to more farmers and faster work processes 	Ethereum, Corda	Belgium, USA, Africa	2018	https://www.forbes.com/sites/michaelcastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8adc30e6
48	Golden States Foods	Food Processing	<ul style="list-style-type: none"> Restaurant supplier is participating in IBM's Food Trust consortium First application: Burger Supply Chain - Control food temperature from meat processors to shippers to restaurants by a blockchain solution to reduce paperwork and food spoilage as well as improving food safety 	IBM Food Trust Blockchain	USA	2019	https://www.forbes.com/sites/michaelcastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8adc30e6
49	Hershey Chocolate Company	Food Processing	<ul style="list-style-type: none"> Biggest Chocolate producer worldwide joins an Blockchain Advertising Consortium "AdLedger" AdLedger was founded by IBM, Tegna, MadHive in 2018 and is a non-profit consortium for blockchain in the digital advertising market Other blockchain developments of Hershey focusing cacao traceability, and optimization of operations in chocolate operations 	IBM Food Trust	USA	2019	https://cointelegraph.com/news/hershey-chocolate-company-joins-blockchain-advertising-consortium
50	FAO, ITU	Governance	<ul style="list-style-type: none"> Pilot for tracking livestock in a blockchain system 		Papua New Guinea	2019	http://www.fao.org/papua-new-guinea/news/detail-events/en/c/1186014/
51	Malaysia	Governance	<ul style="list-style-type: none"> Malaysian State Penang launched blockchain to track agricultural products Initiated by the Ministry of Agriculture and Agro-based Industries 		Malaysia	2019	https://cointelegraph.com/news/malaysian-state-to-launch-blockchain-solution-to-track-agricultural-products-says-official
52	Siemens	IT	<ul style="list-style-type: none"> Blockchain zur Rückverfolgbarkeit und Zertifizierung von Bio-Kartoffelchips zusammen mit Alos IT Solutions and Services GmbH Dabei werden vorhandene, etablierte Systeme wie MindSphere als cloud-basiertes, offenes IoT-Betriebssystem und das Portfolio an kommunikationsfähiger Hardware mit der Blockchain-Technologie verknüpft. 		Deutschland	2019	https://new.siemens.com/global/de/unternehmen/stories/industrie/blockchain-fuer-lebensmittelsicherheit.html
53	WWF, Boston Consulting Group	NPO	<ul style="list-style-type: none"> Launch of the "OpenSC food provenance blockchain" Purpose of the blockchain platform is to ensure products are ethically sourced OpenSC is based on a WWF pilot to trace tuna. 	OpenSC	Australia	2019	https://www.ledgerinsights.com/wwf-boston-consulting-launch-food-provenance-blockchain/ https://open-sc.com/technology.html
54	Metro + Deepshore	Retail	<ul style="list-style-type: none"> Cloudspeicher mit BCT für revisionssichere + gesetzkonforme Dokumentenablage 12 Monate Projektlaufzeit 2019 erfolgreich beendet 50% der Storagekosten durch BCT-Lösung senkbar Ausbau des Systems parallel zum bisherigen Datenbank-/Cloudsystem bei METRO für 2019 geplant 	Deepshore	Deutschland	2019	https://www.presseportal.de/pm/129233/4187199
55	Alibaba, PWC, Blackmores, Australia Post, Fonterra	Retail	<ul style="list-style-type: none"> Cooperation of Alibaba and PWC with AusPost and Blackmores to track food production from farm to fork from Australia and NZ to China 		Australia, New Zealand, China	Apr 18	https://ambcrypto.com/alibaba-and-pwc-work-together-using-blockchain-technology-to-ensure-food-safety/
56	Dairy Farmers of America (DFA) + ripe.io	Animal Protein	<ul style="list-style-type: none"> DFA as major U.S. national milk cooperative, owned by dairy farmers (Net Income 2017: 127.4 Mio. \$ / 30 % of the total national milk production) Technical partner is the BC-StartUp Ripe.io Project focuses the improvement of Supply Chain transparency 	ripe.io-Plattform	USA	Sep 18	https://cointelegraph.com/news/major-us-dairy-co-op-pilots-blockchain-technology-for-food-supply
57	South Korea	Governance	<ul style="list-style-type: none"> Science and AgFood Ministries testing Blockchain to trace beef supply chain Providing consumers detailed and trustworthy information about a product is the main target of this pilot 		South Korea	Nov 18	https://cointelegraph.com/news/south-korea-science-food-ministries-to-use-blockchain-for-tracing-beef-supply-chain
58	Chinese Province Chingping	Governance	<ul style="list-style-type: none"> Pharma and Food Security Agency of Chinese Province Chingping is testing blockchain for a more efficient traceability system 		China	Feb 19	https://de.cointelegraph.com/news/chinese-district-food-and-drug-administration-to-use-blockchain-for-quality-assurance
59	Albertsons	Retail	<ul style="list-style-type: none"> Second largest US-Retailer (u.a. Safeway) Using IBM Food Trust for tracing lettuce as a first BC-Pilot, a roll-out is already announced 	IBM Blockchain	USA	Apr 19	https://cointelegraph.com/news/us-food-retailer-albertsons-uses-ibm-food-trust-blockchain-to-track-lettuce
60	Carrefour + Nestlé + IBM Food Trust	Retail	<ul style="list-style-type: none"> Partnering for tracking instant mashed potatoes of French convenience brand "Mouline" Customers will be able to see exactly where the potatoes in a specific packet came from and get information about it's journey to this Carrefour store by scanning a QR-code on the product's packet. Information includes varieties of potatoes that were used, date and place of manufacture, quality control information and storage date and place 	IBM	France, Switzerland	Apr 19	https://cointelegraph.com/news/nestle-carrefour-work-with-ibm-to-track-mashed-potato-brand-with-blockchain
61	AUCHAN + TE Foods	Retail	<ul style="list-style-type: none"> Partnered with TE-Food for a testing project of TE-Food's BC-platform "Foodchain" in Vietnam (2017-18) Roll-out to five more countries in Dec. 2018: Italy, Spain, Portugal, Senegal, France Traceability solution with records about product quality data, logistics information Customers are able to check a products history by a QR-Code giving access to FoodChain 		France	Dec. 2018	https://cointelegraph.com/news/global-retail-giant-auchan-expands-blockchain-tracking-solution-to-five-more-countries

No.	Company Partner	Typ	Beschreibung	Blockchain-Technologie	Region	Startzeit	Quelle
62	Swedish land ownership authority Lantmäteriet	Governance	<ul style="list-style-type: none"> Land registry and property transaction on blockchain as a pilot Safe and secure way to handle digital originals 		Sweden	Mar. 2018	https://de.cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction
63	Alibaba + JD.com	Retail	<ul style="list-style-type: none"> Blockchain as traceability tool to improve consumer confidence in the authenticity of food products JD.com started tracking beef from Kerchin, an inner Mongolia company to markets in Beijing, Shanghai and Guangzhou Additional cooperation with InterAgri (Australian exporter), HW Greenham & Sons (food processor) to track black angus beef as premium line 	BaaS	China	March 18	https://cointelvet.com/de/china-approves-197-blockchain-firms-inc-alibaba-jd-com/ https://medi.um.com/@Michael_Spencer/the-amazon-of-china-has-adopted-blockchain-to-track-high-end-beef-imports-bf927671191a
64	US National Pork Board	Animal Protein	<ul style="list-style-type: none"> Pilot of the U.S. National Pork Board in partnership with BC Start-up ripe.io to use BCT for pork supply chains They want to use a BC-based platform to monitor and evaluate food safety standards, sustainability practices, livestock health and environmental protections during the production process The platform will provide information about the production of pork, enhancing transparency and ensure valid digital certifications. Information in the system will be anonymous, but enable an immutable, trusted sharing of data that address critical issues such as quality, waste, fraud, environmental impact of pork production, traceability 		USA	March 19	https://cointelegraph.com/news/us-national-pork-board-to-pilot-blockchain-tech-following-new-partnership
65	Bumble Bee Foods + SAP	Food Processing	<ul style="list-style-type: none"> Bumble Bee Foods launched a seafood traceability platform in cooperation with SAP Monitoring the Yellowfin tuna supply chain from Indonesia to supermarkets in the US: size of the catch, point of capture, information about authenticity, freshness, safety, trade fishing certification Target: optimizing food safety and sustainability, instilling confidence in seafood supply chain, which has been targeted by environmental activists for killing dolphins 	Multichain	USA	March 19	https://cointelegraph.com/news/north-american-seafood-firm-to-use-blockchain-tech-in-supply-chain https://www.forbes.com/sites/michaelcastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8adc30e6
66	Coffee Board of India	Governance	<ul style="list-style-type: none"> The Coffee Board is backed by the Indian Ministry of Commerce and Industry (MCI) to promote India's coffee production Launch of a pilot-blockchain-based e-marketplace to reduce the number of intermediaries and integrate farmers directly with relevant markets Additionally target: improvement of supply chain transparency and traceability "from bean to cup" Technical support by M/S Eka Plus, a management software provider for agriculture 		India	March 19	https://cointelegraph.com/news/india-to-use-blockchain-to-improve-coffee-supply-chain
67	Carrefour	Retail	<ul style="list-style-type: none"> Carrefour starting to roll out the blockchain-based "Carrefour Quality Line" with a new product: Micro-filtered full-fat milk, which guarantees consumers a complete traceability across the supply chain Consumers will be able to see GPS coordinates of the farmers whose animals' milk was collected, information about the date when milk was collected and packaged and from whom 	IBM	French	March 19	https://cointelegraph.com/news/retail-giant-carrefour-applies-blockchain-for-tracking-milk-product-supply-chain
68	Coca-Cola	Food Processing	<ul style="list-style-type: none"> Kooperation mit US-Außenministerium Blockchain als Basis für Arbeitsbedingungen in globalen Lieferketten für Zucker von Coca-Cola Coca-Cola hat Studie mit Thomson Reuters zugestimmt, um Zwangsarbeit, Kinderarbeit usw. in deren Lieferketten zu untersuchen und gibt dafür Daten preis. 		USA	March 2018	https://www.foia.de/2018/03/27/coca-cola-nutzt-die-blockchain-zur-verbesserung-der-arbeitnehmerrechte/ https://www.reuters.com/article/us-blockchain-coca-cola-labor/coca-cola-u-s-state-dept-to-use-blockchain-to-combat-forced-labor-idUSKCN1G52PY
69	Frievær, AgOS, For Farmers, MS Schippers, Topigs Norsvin, De Varkenspraktijk	Konsortium	<ul style="list-style-type: none"> Abschluss eines Pilotprojektes zur Rückverfolgbarkeit und Nachweis über Produktionschwerpunkte Abbildung kompletter Schweinefleischketten (Genetik, Herkunft, Futtermittel, Tierarztbesuche, Transport- und Schlachtdaten) Erstellung eines digitalen Schweinepasses zu jedem Stück Fleisch mit diesen Informationen Projektstart November 2018 Fokus auf Rückverfolgbarkeit, Prozessverbesserung durch Transparenzschaffung und Garantie für hohe Qualität und Lebensmittelsicherheit (Mehrwert in Kontrollierbarkeit und Rückverfolgbarkeit für Kettenpartner und Endkunden) 	AgOS stellt Plattform bereit	Niederlande	Nov. 18 - Mai 19	https://www.forfarmers.nl/media/blockchain-voor-frievær-variantenlees-is-een-feit.aspx
70	Cargill + Intel	Commodity	<ul style="list-style-type: none"> Turkey Supply Chain as first pilot for testing the potential of blockchain to track and trace a whole food supply chain 70 Turkey farms in Texas and Missouri, 3500 supermarkets were involved to track 200.000 Turkeys by a blockchain-solution Cargill also joins a team of engineers together with Intel and enterprise startup Bitwise to build Hyperledger Grid - for tracking food back to its origin 	Hyperledger Sawtooth, Hyperledger Grit	USA	Oct. 2017	https://www.agrarzeitung.de/nachrichten/wirtschaft/transparenz-truthahn-in-der-blockchain-85229?refresh=1
71	Albert Heijn	Retail	<ul style="list-style-type: none"> Pilot to make the orange juice production transparent for customers Albert Heijn (Holland's largest supermarket chain) partners with it's supplier Refresco and Louis Dreyfus Company to trace the journey of Orange Juice from Netherlands back to its origin in Brazil Focus on sustainable production, quality information as well as ingredients, Albert Heijn and Customers will be able to know the grower's quality certifications for food safety and sustainability. Customers can compliment farmers by providing feedback. Starting in April 2019 to trace "Beter Leven"-certified eggs in a blockchain, planning to develop a blockchain-based traceability system for all fresh-products until 2025 		Netherlands	Sept. 18 Apr. 19	https://www.crysto-insiders.nl/nieuws/albert-heijn-gebruikt-blockchain-voor-transparantere-productieketen/ https://www.ledgerinsights.com/supermarket-albert-heijn-blockchain-food-traceability/
72	BP PLC	Commodity	<ul style="list-style-type: none"> Increasing the efficiency of commodities trade finance BP has invested more than \$20 Million in blockchain projects 	Ethereum, Cardano, Quorum	Großbritannien		https://www.forbes.com/sites/michaelcastillo/2019/04/16/blockchains-billion-dollar-babies/#2a1d8adc30e6
73	Cargill Risk Management	Commodity	<ul style="list-style-type: none"> Cargill Risk Management is testing blockchain to create immutable land titles to prove ownership and protect farmers from corruption Digitalization of paper-based contracts into "smart contracts" to improve efficiency and minimize costs, increasing transparency. 		USA		https://books.google.de/books?id=d8-HDwAAQBAJ&pg=PA52&pg=PA52&dq=Cargill+Risk+Management+Blockchain&source=bl&ots=9umRSaJ_XQ&sig=ACU3U23Jn8RD0mniYwWFA3X2exNH2A&hl=de&sa=X&ved=2ahUKEwjrtqV-fThXQb1AKHxm_A50Q6AEwCHoECAlQAQ#v=onepage&q=Cargill%20Risk%20Management%20Blockchain&f=false
74	BeefChain	Start-Up	<ul style="list-style-type: none"> Wyoming cattle ranchers founded this alliance to track beef along the supply chain and to recapture value from third party actors Target: ranchers wanted to know where their beef was sold Beefchain is certified by USDA since April 2019 as trust programme for better production: Non-Hormone treated cattle, BeefChain Natural (non Hormones, antibiotics, ionophores), BeefChain Wyoming+ (pasture raised, born in Wyoming), Age and Source Verification (immutable proof of individual cattle age and where cattle was born and raised) 	TE-Foods	USA	2018	https://www.tdn.com/news/asdasda-291/

No.	Company Partner	Typ	Beschreibung	Blockchain-Technologie	Region	Startzeit	Quelle
75	BEXT360	Start-Up	<ul style="list-style-type: none"> • Proof of sustainable production by transparency • Combination of visual assaying and weighing and blockchain for coffee trading • Technology allows buyer to rapidly analyze the quality of a farmers coffee in the field and weight it. • According to the quality farmer and buyer are able to negotiate a fair price on the bext360 mobile app • The combination of reliable trading and blockchain allows Bext360 to aspire to bring complete transparency to the coffee supply chain, palm oil, Sea fruits, timber, cotton and other critical supply chains 	BaaS - BextMachine	USA	2018	https://blockchainwelt.de/bext360-von-der-blockchain-zum-kaffee/ https://www.bext360.com/
76	Syngenta, Accenture, GEB	Insurance	Employer Benefits		Switzerland, Spain, Serbia	2018	https://www.forbes.com/sites/lukefitzpatrick/2019/04/16/syngenta-and-accenture-debut-a-new-blockchain-solution/#3ca782b73e93
77	Demeter	Start-Up	• A central hub to rent and farm micro fields anywhere in the world. Focusing the disintermediation and complexity as well as the overhead costs	Ethereum		2016	https://www.startup-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-agricultural-industry/ https://demeter.life/
78	Bin Kabi						
79	Viant	Start-Up	<ul style="list-style-type: none"> • BC-based platform for tracking assets and building future supply chains • Management of assets through the entire value chain based on smart contracts • Pilot with WWF, another Pilot with the world economic forum 	Consensys, Ethereum based	USA	2018	https://viant.io/
80	Etherisc	Start-Up	• Offering Crop insurance to farmers by a decentralized insurance application		Deutschland		https://www.startup-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-agricultural-industry/
81	Worldcover	Start-Up	• Provide crop insurance to protect against loss of yield using satellites to monitor rainfall and trigger payouts automatically		USA		https://www.startup-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-agricultural-industry/
82	Avenews-GT	Start-Up	<ul style="list-style-type: none"> • Digital trading platform enables verified agri-businesses, farmers, cooperatives and commercial agri-buyers to transact directly with each other locally and worldwide • Reduction of transaction costs, financial security and optimized transparency of Supply Chains 		Israel		
83	Coffee Coin	Start-Up	<ul style="list-style-type: none"> • CoffeeCoin (COF) Is The World's 1st Token For Buying, Selling & Tracking Coffee Using Distributed Ledger Technology On The Waves Platform • CoffeeCoin ist eine Handelsplattform für den globalen Kaffeemarkt, über die Kaffeebauern ihre Produkte ohne Zwischenhändler direkt an den Endkunden bringen können. Gründer James Allen war 2013 einer der ersten, der Kaffee gegen Bitcoin anbot. Inzwischen erfolgt der Handel auf CoffeeCoin in der gleichnamigen Kryptowährung. 		Malaysia	2017	https://www.gruendenszene.de/galerie/krypto-und-food?pid=16668 https://coffeecoin.io/
84	Civic	Start-Up	Der Krypto-Bierautomat des US-Startups Civic soll das Alter der Kunden mithilfe der Blockchain überwachen. Bevor das Gerät ein Getränk ausgibt, überprüft es, ob der potenzielle Käufer alt genug ist. Dafür müssen die Käufer ihren Ausweis über die Civic-App verifizieren lassen. Für den Automaten arbeitet das Startup mit der Brauereigruppe Anheuser-Busch zusammen, die Marken wie Stella Artois und Budweiser vertreibt.		USA		
86	Lokaal Market	Start-Up	Direct Sales by 1st own Cryptocurrency, targeting the creation of a money market for critical businesses		USA		
87	AgriChain	Start-Up	Focus on enabling Peer-to-Peer Agricultural Transactions and processing, disintermediation of middlemen		Australien		https://agrichain.com/
88	AgriUnity	Start-Up	Using Distributed Cryptolledger And Mobile Apps To Create A Circle Of Trust For Small Farmer Co-Operatives .		Australien		
89	FoodCoin Ecosystem	Start-Up	The FOODCOIN ECOSYSTEM deals will take place with the use of smart contracts, while the transactions will accept a proper cryptocurrency named FoodCoin (FOOD). A wide selection of tools, such as a proper "smart" wallet, a remote user identification system, flexibly configurable smart contracts, authentication of the origin of food and a proper crypto payment processor, will let the business process participants related to food choose and customize the essential platform parameters to reduce current expenses. A significant potential may be in using FoodCoin Ecosystem in social projects. FOODCOIN ECOSYSTEM has the plans to support food and ag startups with the verified model, innovation content and the significant growth potential using the platform of 1000EcoFarms and FCE blockchain. The special crypto fund will be founded with this aim of view. The purpose of fund will be an effective use of liquid money to build an integral ecosystem.		Switzerland	2017	https://medium.com/lokaal/12-blockchain-food-agriculture-companies-in-their-own-words-7118398252eb
90	Kraft Heinz, Evolv, Ministry of Ag, Food, Forestry, Tourism Policy)	Food Processing	Plasmon, Kraft's Italian Brand for Children's Food partners with the MIPAAFT to enhance food safety for kids. They want to test Blockchain for an optimized traceability of food, beside the application of blockchain the project target is to develop a verification system for quality and safety of children's food as well as a promotion of "Made in Italy"	Evolv	Italy	Mal 19	https://www.ledgerinsights.com/kraft-heinz-blockchain-baby-food-traceability-plasmon/

Literaturverzeichnis

- Adolph, M.; Narayan, A.; Eskandar, H. und Mandahar, S. (2019): Blockchain: Understanding the implementation risks. In: Gerard, S. (Hg.): E-Agriculture in Action: Blockchain for Agriculture. Opportunities and Challenges. Bangkok, S. 11–18. Online verfügbar unter <http://www.fao.org/3/CA2906EN/ca2906en.pdf>, zuletzt geprüft am 24.04.2019.
- Angelis, S.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A. und Sassone, V. (2017): Pbft Vs Proof-Of-Authority: Applying The Cap Theorem To Permissioned Blockchain.
- Antonopoulos, A. M. (2017): Mastering Bitcoin. Programming the open Blockchain. Sebastopol, O'Reilly Media. Online verfügbar unter <http://proquest.tech.safaribooksonline.de/9781491954379>, zuletzt geprüft am 20.05.2019.
- Antonopoulos, A. M. (2018): Bitcoin und Blockchain - Grundlagen und Programmierung. Die Blockchain verstehen, Anwendungen entwickeln. Heidelberg: O'Reilly. Online verfügbar unter <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1804640>, zuletzt geprüft am 24.05.2019.
- Baliga, A. (2017): Understanding Blockchain Consensus Models. Santa Clara: Persistent Systems Ltd. Online verfügbar unter <https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf>, zuletzt geprüft am 20.05.2019.
- Bayer, D.; Haber, S. und Stornetta, W.S. (1993): Improving the Efficiency and Reliability of Digital Time-Stamping. In: Sequences II: Methods in Communication, Security and Computer Science, S. 329–334, Online verfügbar unter <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.4891&rep=rep1&type=pdf>, zuletzt geprüft am 20.05.2019.
- Bogensperger, A.; Zeiselmaier, A. und Hinterstocker, M. (2018): Die Blockchain-Technologie: Chance zur Transformation der Energieversorgung? Berichtsteil: Technologiebeschreibung. München: FFE, Online verfügbar unter https://www.ffe.de/attachments/article/803/Blockchain_Teilbericht_Technologiebeschreibung.pdf, zuletzt geprüft am 30.07.2019.
- Boyle, B.; Brenner, A.; Steger, S.; Janssen, S. und Rasamoela, M. (2018): The blockchain bandwagon. Is it time for automotive companies to start investing seriously in blockchain?. München: Roland Berger, Online verfügbar unter https://www.rolandberger.com/publications/publication_pdf/roland_berger_blockchain_automotive.pdf, zuletzt geprüft am 03.09.2019
- Brandt, J.; Hoffknecht, A. und Krug, C. (2018): Blockchain Technologie: Anwendungsfelder und limitierende Faktoren. In: VDI Technologiezentrum (Hrsg.): Blockchain - Eine Technologie mit disruptivem Charakter. Düsseldorf: VDI publishing house, S. 11–14.
- Brown, R.G. (2015): A simple model for Smart Contracts. Online verfügbar unter <https://gandal.me/2015/02/10/a-simple-model-for-smart-contracts/>, zuletzt geprüft am 30.07.2019.
- Buchmann, J.; Dahmen, E.; Klintsevich, E.; Okeya, K. und Vuillaume, C. (2007): Merkle Signatures with Virtually Unlimited Signature Capacity. In: Jonathan, K. und Moti, Y. (Hg.): Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 31–45.

- Buntinx, J. P. (2017): What is Delegated Byzantine Fault Tolerance? Hg. v. The Merkle. Soquel, USA. Online verfügbar unter <https://themerkle.com/what-is-delegated-byzantine-fault-tolerance/>, zuletzt geprüft am 10.05.2019.
- Burgwinkel, D. (2016): Blockchain technology. Einführung für Business- und IT Manager. Berlin, Boston: De Gruyter Oldenbourg. Online verfügbar unter http://www.degruyter.com/search?f_0=isbnissn&q_0=9783110487312&searchTitles=true, zuletzt geprüft am 03.09.2019
- Buterin, V. (2014): Ethereum – A Next-Generation Cryptocurrency and Decentralized Application Platform. Hg. v. Bitcoin Magazine. Online verfügbar unter <https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211>, zuletzt geprüft am 30.07.2019.
- Carbone, A.; Davcev, D.; Mitreski, K.; Kocarev, L. und Stankovski, V. (2018): Blockchain based Distributed Cloud Fog Platform for IoT Supply Chain Management. In: Eighth International Conference On Advances in Computing, Electronics and Electrical Technology - CEET 2018: Institute of Research Engineers and Doctors, S. 51–58.
- Caro, M. P.; Ali, M. S.; Vecchio, M. und Giaffreda, R. (2018): Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In: IoT Vertical and Topical Summit on Agriculture, Toskana: IEEE, S. 1–4.
- Casado-Vara, R.; Prieto, J.; La Prieta, F. und Corchado, J.M. (2018): How blockchain improves the supply chain: case study alimentary supply chain. In: Procedia Computer Science 134, S. 393–398. DOI: 10.1016/j.procs.2018.07.193.
- Castro, M. und Liskov, B. (1999): Practical Byzantine Fault Tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation. Berkeley, CA, USA: USENIX Association, S. 173–186. Online verfügbar unter <http://dl.acm.org/citation.cfm?id=296806.296824>, zuletzt geprüft am 30.04.2019
- Certivation GmbH (2019): Blockchain Ensured Certificates. Online verfügbar unter <https://www.certivation.com/de/services/Seiten/Blockchain-Service.aspx#function>, zuletzt geprüft am 18.08.2019.
- Condos, J.; Sorrell, W. H. und Donegan, S. L. (2016): Blockchain Technology: Opportunities and Risks. Online verfügbar unter <http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf>, zuletzt geprüft am 30.07.2019.
- DeRose, C. (2016): BankThink 'Smart Contracts' Are the Future of Blockchain. American Banker. Online verfügbar unter <https://www.americanbanker.com/opinion/smart-contracts-are-the-future-of-blockchain>, zuletzt geprüft am 03.09.2019.
- Diffie, W. und Hellman, M. (1976): New directions in cryptography. In: IEEE Trans. Inform. Theory 22 (6), S. 644–654. DOI: 10.1109/TIT.1976.1055638.
- Drescher, D. (2017): Blockchain Grundlagen. Eine Einführung in die elementaren Konzepte in 25 Schritten. Frechen: mitp (mitp Business). Online verfügbar unter <https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5123641>, zuletzt geprüft am 03.09.2019.
- Drösser, C. (2019): Problem gelöst – in rund drei Minuten statt 10.000 Jahren. Hg. v ZEIT Online. Online verfügbar unter: <https://www.zeit.de/digital/datenschutz/2019-09/quantencomputer-google-technik-fortschritt-supercomputer>, zuletzt geprüft am 10.10.2019.

- Düring, T. und Fisbeck, H. (2017): Einsatz der Blockchain-Technologie für eine transparente Wertschöpfungskette. In: Hildebrandt, A.; Landhäußer, W. (Hrsg.): CSR und Digitalisierung. Der digitale Wandel als Chance und Herausforderung für Wirtschaft und Gesellschaft. Berlin, Heidelberg: Springer Gabler, S. 449–464.
- Edelman (2018): Edelman trust barometer. Executive summary. Online verfügbar unter https://www.edelman.de/fileadmin/user_upload/Magazin_-_Studien_Insights/2018_Edelman_Trust_Barometer_Executive_Summary_-_Jan.pdf, zuletzt geprüft am 10.09.2019.
- Eickmeyer, S. C.; Halaszovich, T. und Lattemann, C.: Blockchain Technologien für die Sicherung von Material-, Informations- und Geldflüssen in der Logistik. Erfolgsfaktoren für die chinesische „Belt-Road“ Initiative. In: HMD (2018) 55: 1260-1273, Wiesbaden: Springer Fachmedien GmbH, DOI: 10.1365/s40702-018-00465-7.
- Foamspace Corp (2018): FOAM Whitepaper. Online verfügbar unter https://www.foam.space/publicAssets/FOAM_Whitepaper.pdf, zuletzt geprüft am 10.08.2019.
- Förster, M. (2019): Blockchain: Dem Marketing-Hype auf die Finger geschaut. Hg. v. Heise Online: iX Magazin. Online verfügbar unter <https://www.heise.de/ix/meldung/Blockchain-Dem-Marketing-Hype-auf-die-Finger-geschaut-4512654.html>, zuletzt aktualisiert am 03.09.2019, zuletzt geprüft am 26.09.2019.
- Franco, P. (2014): Understanding Bitcoin. Chichester, UK: John Wiley & Sons, Ltd.
- Glaser, F. und Bezenberger, L. (2015): Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems. In: Proceedings of the 23rd European Conference on Information Systems, ECIS 2015, Münster: Universität Münster. Online verfügbar unter <https://pdfs.semanticscholar.org/ac2c/c809d7b2125b6557fcd73d5faddba710e948.pdf>, zuletzt geprüft am 10.03.2019
- GS1 Innovation (2018): Was kann Blockchain wirklich? Ergebnisse aus dem Pilotprojekt "Palettentausch mit Blockchain-Technologie". Hg. v. GS1 Germany GmbH. Online verfügbar unter https://www.gs1-germany.de/fileadmin/gs1/basis_informationen/was_kann_blockchain_wirklich.pdf, zuletzt aktualisiert am 2018, zuletzt geprüft am 10.05.2019.
- Gupta, M. (2017): Blockchain For Dummies. Hg. v. IBM Limited Edition. Wiley. Hoboken.
- Hackius, N. und Petersen, M. (2017): Blockchain in logistics and supply chain. Trick or treat? In: Kersten, W.; Blecker, T. und Ringle, C.M. (Hg.): Digitalization in supply chain management and logistics. Hamburg International Conference of Logistics. Hamburg: epubli GmbH, S. 3–18.
- Hammerschmidt, C. (2017): Consensus in Blockchain Systems. In Short. San Francisco: Medium. Online verfügbar unter <https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe>, zuletzt geprüft am 30.07.2019.
- Hermes Germany GmbH (2018): Kollaboration in der Supply Chain. Online verfügbar unter <https://www.hermes-supply-chain-blog.com/wp-content/uploads/2018/11/18-1106-Hermes-Newsletter-web.pdf>, zuletzt geprüft am 01.08.2019.

- Herwlijer, C.; Waughray, D. und Warren, S. (2018): Building bock(chain)s for a better planet. Hg. v. World Economic Forum. Online verfügbar unter http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf, zuletzt geprüft am 01.08.2019.
- Hinckeldeyn, J. (2019): Blockchain-Technologie in der Supply Chain. Einführung und Anwendungsbeispiele (essentials). Online verfügbar unter <https://doi.org/10.1007/978-3-658-26440-6>, zuletzt geprüft am 05.09.2019.
- Horstmann, J. (2016): Kommunikationssysteme und Farming 4.0 in der Landtechnik. Braunschweig: Institut für mobile Maschinen und Nutzfahrzeuge. Online verfügbar unter https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00055103, zuletzt geprüft am 22.10.2019.
- Hoskinson, C. (2018): Cardano Settlement Layer Documentation. Online verfügbar unter <https://cardanodocs.com/introduction/>, zuletzt geprüft am 04.09.2019.
- Hosp, J. (2018): Blockchain 2.0. Einfach erklärt - weit mehr als nur Bitcoin. München: FBV.
- Hyperledger Sawtooth (2018): Revolutionizing the Supply Chain. Bringing traceability and accountability to the supply chain through the power of Hyperledger Sawtooth's distributed ledger technology. Online verfügbar unter <https://sawtooth.hyperledger.org/examples/seafood.html>, zuletzt geprüft am 20.08.2019.
- IBM Food Trust (2019): About IBM Food Trust. IBM Limited Edition. Online verfügbar unter <https://www.ibm.com/downloads/cas/EX1MA1OX>, zuletzt geprüft am 10.08.2019.
- Ivica, N.; Aashish, K.; Ilya, S.; Prateek, S. und Aquinas, H. (2018): Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. In: Annual Computer Security Applications Conference (ACSAC '18), S. 653–664. Online verfügbar unter <http://delivery.acm.org/10.1145/3280000/3274743/p653-nikolic.pdf> , zuletzt geprüft am 20.04.2019.
- Juels, A.; Kosba, A. und Shi, E. (2015): The Ring of Gyges: Using Smart Contracts for Crime. Online verfügbar unter <http://www.arjuels.com/wp-content/uploads/2013/09/Gyges.pdf>, zuletzt geprüft am 05.09.2019.
- Kandel, C.; Klumpp, M. und Keusgen, T. (2011): GPS based track and trace for transparent and sustainable global supply chains. In: Thoben, K.D. (Hg.): 17th International Conference on Concurrent Enterprising. ICE. Aachen: Forschungsinstitut für Rationalisierung e.V. an der RWTH Aachen.
- Kendall, H.; Naughton, P.; Kuznesof, S.; Raley, M; Dean, M and Clark, B. (2018)cFood fraud and the perceived integrity of European food imports into China. In: PLoS ONE 13(5):e0195817. Online verfügbar unter <https://doi.org/10.1371/journal.pone.0195817>, zuletzt geprüft am 20.10.2019.
- Klenk und Hoursch (2011): Warum müssen Unternehmen transparent sein? Hg. v. Statista. Online verfügbar unter <https://de.statista.com/statistik/daten/studie/196026/umfrage/meinung-zur-notwendigkeit-von-transparenz-von-unternehmen/>, zuletzt geprüft am 20.09.2019.

- Kückelhaus, M.; Chung, G.; González-Peralta, J.; Turner, K.; Gockel, B.; Acar, T. (2018): Blockchain in Logistics. Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. Hg. v. DHL Customer Solutions & Innovation in Cooperation with Accenture Consulting. Online verfügbar unter <https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf>, zuletzt geprüft am 26.09.2019.
- Leong, C.; Viskin, T. und Steward, R. (2018): Tracing the Supply Chain. How blockchain can enable traceability in the food industry. Hg. v. Accenture. Online verfügbar unter https://www.accenture.com/_acnmedia/PDF-93/Accenture-Tracing-Supply-Chain-Blockchain-Study-PoV.pdf, zuletzt geprüft am 24.04.2019.
- Lin, J.; Shen, Z.; Zhang, A. und Chai, Y. (2018): Blockchain and IoT based Food Traceability for Smart Agriculture. In: Proceedings of the 3rd International Conference on Crowd Science and Engineering - ICCSE'18. Singapore, New York: ACM Press, S. 1–6.
- Manoury, P. (2007): Functional programming, inductive data types and proofs. Université Pierre et Marie CURIE. Paris. Online verfügbar unter <https://www.irif.fr/~eleph/Enseignement/c-tbilisi.pdf>, zuletzt geprüft am 15.04.2019.
- Mattila, J. (2016): The Blockchain Phenomenon. The Disruptive Potential of Distributed Consensus Architectures. In: ETLA Working Papers. Online verfügbar unter <https://ideas.repec.org/p/rif/wpaper/38.html>, zuletzt geprüft am 30.07.2019.
- Meinel, C.; Gayvoronskaya, T. und Schnjakin, M. (2018): Blockchain. Hype oder Innovation. Potsdam: Universitätsverlag Potsdam (Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam, 113). Online verfügbar unter <http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-103141>, zuletzt geprüft am 24.04.2019.
- Merkle, R.C. (1990): A Certified Digital Signature. In: Brassard, G. (Hrsg.): Advances in Cryptology. New York: Springer New York, S. 218–238.
- Meunier, S. (2018): When do you need blockchain? Decision models. Hg. v. Medium. Online verfügbar unter <https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1>, zuletzt geprüft am 26.09.2019.
- Morrison, A. (2016): How smart contracts automate digital business. Hg. v. PWC. Online verfügbar unter <http://usblogs.pwc.com/emerging-technology/how-smart-contracts-automate-digital-business/>, zuletzt geprüft am 30.07.2019.
- Mougayar, W. und Buterin, V. (2016): The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology: Wiley. Online verfügbar unter <https://books.google.de/books?id=CEsPDAAAQBAJ>, zuletzt geprüft am 21.09.2019.
- Mullender, S.J. (1995): Distributed systems. New York: ACM Press (ACM Press frontier series).
- Müller, M. und Bessas, Y. (2017): Potenzialen von Brancheninitiativen zur nachhaltigen Gestaltung von Liefer- und Wertschöpfungsketten – Studie. Bundesministerium für Arbeit und Soziales, Universität Ulm, Ulm.
- Nakamoto, S. (2009): Bitcoin: A Peer-to-Peer Electronic Cash System. Online verfügbar unter <https://bitcoin.org/bitcoin.pdf>, zuletzt geprüft am 02.04.2019.

- Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A. und Goldfeder, S. (2016): Bitcoin and cryptocurrency technologies. A comprehensive introduction. Princeton: Princeton University Press.
- Olson, K.; Bowman, M.; Mitchell, J.; Amundson, S.; Middleton, D. und Montgomery, C. (2018): Sawtooth: An Introduction. Online verfügbar unter https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf, zuletzt geprüft am 20.08.2019.
- Oram, A. (2001): Peer-to-Peer: Harnessing the Power of Disruptive Technologies: O'Reilly Media. Online verfügbar unter <https://books.google.de/books?id=Vh-SCgAAQBAJ>, zuletzt geprüft am 03.09.2019
- Paar, C.; Pelzl, J. und Preneel, B. (2010): Understanding cryptography. A textbook for students and practitioners. 2nd corrected printing. Berlin: Springer.
- Palka, S. und Wittpahl, V. (2018): Vertrauen und Transparenz - Blockchain-Technologie als digitaler Vertrauenskatalysator. In: Wittpahl, H. (Hrsg.): iit perspektive, 39. Berlin: Institut für Innovation und Technik iit.
- Peck, M.E. (2017): Do You Need a Blockchain? In: IEEE Spectrum. Online verfügbar unter <https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain>, zuletzt geprüft am 26.09.2019.
- Prusty, N. (2017): Building blockchain projects. Building decentralized blockchain applications with Ethereum and Solidity. Birmingham, Mumbai: Packt.
- Rosenberger, P. (2018): Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Berlin: Springer Vieweg. Online verfügbar unter <http://dx.doi.org/10.1007/978-3-662-56088-4>, zuletzt geprüft am 03.09.2019
- Sallaba, M.; Siegel, D. und Becker, S. (2018): IoT powered by Blockchain. How Blockchains facilitate the application of digital twins in IoT. Hg. v. Deloitte. Online verfügbar unter <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/IoT-powered-by-Blockchain-Deloitte.pdf>, zuletzt geprüft am 18.03.2019.
- Sanders, R. (2006) A market road to sustainable agriculture? Ecological agriculture, green food and organic agriculture in China. In: Development and Change, 37. Blackwell Publishing, S. 201–226.
- Schiller, K. (2018): FOAM – Proof of Location Protokoll erklärt. Hg. v. Blockchain Welt. Online verfügbar unter <https://blockchainwelt.de/foam-proof-of-location-protokoll/>, zuletzt geprüft am 13.08.2019.
- Schlatt, V.; Schweizer, A.; Urbach, N. und Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. White Paper. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. Bayreuth. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf, zuletzt geprüft am 02.04.2019.
- Schoder, D. und Fischbach, K. (2002): Peer-to-Peer. In: Wirtschaftsinformatik 44 (6), S. 587–589. DOI: 10.1007/BF03250877.

- Schütte, J.; Fridgen, G.; Prinz, W. ; Rose, T.; Urbach, N. und Hoeren, T. (2017): Blockchain und Smart Contracts. Technologien, Forschungsfragen und Anwendungen. Hg. v. Fraunhofer-Gesellschaft. Online verfügbar unter <http://publica.fraunhofer.de/documents/N-480276.html>, zuletzt aktualisiert am 02.04.2019.
- Schwarzkopf, J.; Adam, K. und Wittenberg, S. (2018): Vertrauen in nachhaltigkeitsorientierte Audits und in Transparenz von Lieferketten – Schafft die Blockchain-Technologie einen Mehrwert? In: Kahre (Hrsg.), Marktorientiertes Produkt- und Produktionsmanagement in digitalen Umwelten. Wiesbaden: Springer Fachmedien GmbH.
- Strüker, J. (2017): Blockchain in der Energiewirtschaft. Potenziale für Energieversorger. Hg. v. bdew - Bundesverband der Energie- und Wasserwirtschaft e.V.. Online verfügbar unter https://www.bdew.de/media/documents/BDEW_Blockchain_Energiewirtschaft_10_2017.pdf, zuletzt geprüft am 15.06.2019.
- Swan, M. (2015): Blockchain. Blueprint for a new economy. Beijing: O'Reilly (Safari Tech Books Online). Online verfügbar unter <http://proquest.safaribooksonline.com/9781491920480>, zuletzt geprüft am 03.09.2019
- Swanson, T. (2014): Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management. Online verfügbar unter <https://s3-us-west-2.amazonaws.com/chainbook/Great+Chain+of+Numbers+A+Guide+to+Smart+Contracts%2C+Smart+Property+and+Trustless+Asset+Management+-+Tim+Swanson.pdf>, zuletzt geprüft am 30.05.2019.
- Swanson, T. (2015): Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Online verfügbar unter <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>, zuletzt geprüft am 10.04.2019.
- Tanenbaum, A. S. und van Steen, M. (2016): Distributed Systems: Principles and Paradigms: Create Space Independent Publishing Platform. Online verfügbar unter <https://books.google.de/books?id=qhWZjwEACAAJ>, zuletzt geprüft am 23.09.2019
- Tapscott, D. und Tapscott, A. (2018): Die Blockchain Revolution. Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert. Kulmbach: Plassen Verlag.
- Tian, F. (2016): An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th International Conference, S. 1–6.
- Tradelens (2018): Solution Brief. Online verfügbar unter <https://docs.tradelens.com/>, zuletzt geprüft am 20.07.2019.
- Tripoli, M. und Schmidhuber, J. (2018): Emerging Opportunities for Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. FAO and ICTSD. Rome and Geneva.
- Tuesta, D.; Alonso, J.; Vegas, I.; Cámara, N.; Pérez, M. L.; Urbiola, P. und Sebastián, J. (2015): Smart contracts: the ultimate automation of trust? Hg. v. BBVA Research (Digital Economy Outlook). Online verfügbar unter https://www.bbva.com/wp-content/uploads/en/2016/11/Digital_Economy_Outlook_Oct15_Cap1.pdf, zuletzt geprüft am 30.07.2019.

- Velthuis, A.G.J.; Unnevehr, L.J.; Hogeveen, H. und Huirne, R.B.M. (2003): New Approaches to Food-Safety Economics.
- Voshmgir, S. (2016): Blockchains, Smart Contracts und das Dezentrale Web. In: Hammel, C. (Hrsg.): Technologiestiftung Berlin. Berlin. Online verfügbar unter https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf, zuletzt geprüft am 15.05.2019.
- Vries, A. (2018): Bitcoin's Growing Energy Problem. In: Joule 2 (5), S. 801–805. DOI: 10.1016/j.joule.2018.04.016.
- Walport, M. (2015): Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser. Online verfügbar unter https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, zuletzt geprüft am 1005.2019.
- Wang, L.; Shen, X.; Li, J.; Shao, J. und Yang, Y. (2019): Cryptographic primitives in blockchains. In: Journal of Network and Computer Applications 127, S. 43–58. DOI: 10.1016/j.jnca.2018.11.003.
- Whalley, S. (2018): IoT & Sensors & Blockchain: The Potential of Real Time Conditions Monitoring the Lifecycle of Food. World Agri-Tech Innovation Summit. San Francisco. Online verfügbar unter <https://futurefoodtechsf.com/wp-content/uploads/2018/03/Steve-Whalley-Advisor-to-Ripe.io-Blockchain-Briefing.pdf>, zuletzt geprüft am 20.08.2019.
- Wright, A. und Filippi, P. (2015): Decentralized Blockchain Technology and the Rise of Lex Cryptographia. In: SSRN Journal. DOI: 10.2139/ssrn.2580664.
- Wu, H.; Li, Z.; King, B.; Ben Miled, Z.; Wassick, J. und Tazelaar, J. (2017): A Distributed Ledger for Supply Chain Physical Distribution Visibility. In: Information 8 (4), S. 137. DOI: 10.3390/info8040137.
- Zamani, M.; Movahedi, M. und Raykova, M. (2018): Rapid-Chain: Scaling Blockchain via Full Sharding. In: ACM SIGSAC Conference on Computer and Communications Security (CCS '18), Toronto, New York: ACM. Online verfügbar unter: <https://doi.org/10.1145/3243734.3243853>, zuletzt geprüft am 10.09.2019.