Nicklas T. Urban

Blockchain for Business

Erfolgreiche Anwendungen und Mehrwerte für Netzwerkteilnehmer identifizieren

Springer Gabler

Blockchain for Business

Nicklas T. Urban

Blockchain for Business

Erfolgreiche Anwendungen und Mehrwerte für Netzwerkteilnehmer identifizieren

Springer Gabler

Nicklas T. Urban
Berlin, Deutschland

ISBN 978-3-658-29821-0 ISBN 978-3-658-29822-7 (eBook)
https://doi.org/10.1007/978-3-658-29822-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Guido Notthoff
Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Mit Blockchain existiert eine neue Technologie, die die gesamte Welt fundamental verändert. Von der Wirtschaft, dem sozialen Zusammenleben bis hin zur Art und Weise wie Demokratie heute funktioniert.

Oder, Blockchain ist einfach nur ein überhypter Technologie-Trend, von dem in einigen Jahren kein Mensch mehr spricht.

Die Meinungen Rund um die Zukunft dieser Technologie sind mindestens genauso kontrovers und divers wie das Wissen Rund um die Funktionsweise, technische Basis, sinnvolle Anwendungsfälle und Mehrwerte.

Doch der Kern der Wahrheit steht zwischen diesen beiden Aussagen. Als ich 2016 begann, mich intensiver mit der neuen Technologie zu beschäftigen, war mir schnell klar wie vielfältig die einzelnen Implementierungen und davon abhängig auch die Anwendungsfälle und Mehrwerte gestrickt sind. Seit 2017 berate ich Unternehmen diverser Branchen zum Thema Blockchain. Begonnen bei einer Einführung in die Architektur und Funktionsweise, über die gemeinsame Diskussion und Ausgestaltung gezielter Einsatzgebiete, bis hin zur technischen Umsetzung individueller Lösungen. Die Frage- und Problemstellungen sind sehr divers, wobei ich bei fast jedem Kunden auf einen Pool kongruenter Fragen und Mythen gestoßen bin, u. a.:

- in einer Blockchain sind alle Daten öffentlich und für den Betrieb werden riesige Rechenzentren benötigt
- jeder Anwendungsfall ist sinnvoll, sobald Daten gespeichert und geteilt werden sollen
- wir setzen auf Blockchain als Technologie-Basis, weil es meine Konkurrenten/Partner machen bzw. noch Innovationsbudget vorhanden ist
- die Blockchain bringt mir keinen Mehrwert, bzw. macht nur Sinn, wenn Vertrauen benötigt wird

Kundenspezifisch habe ich diese und viele weitere Punkte einzeln erläutert, diskutiert und mögliche Lösungsszenarien aufgezeigt. Doch letztendlich haben mich die wiederkehrenden Frage- und Problemstellungen dazu bewegt, eine Lösung zu entwickeln, die ein Großteil dieser Herausforderungen mittels einfacher, dennoch ganzheitlicher Modelle abdeckt und beantwortet. Zunächst als Master-Thesis entwickelt, möchte ich das Wissen und die Modelle in einer grundlegend überarbeiteten Version jetzt gerne als Fachbuch weitergeben. Das Anliegen dieses Buches ist es, Ansprechpartnern und Entscheidern aus den Fach- und Innovationsbereichen den Einstieg in die Blockchain-Technologie zu erleichtern sowie eine konkrete Grundlage für die eigenständige Planung und Evaluation für das Blockchain-Vorhaben im eigenen Unternehmen zu bieten.

Konkret finden Sie in diesem Buch:

- Umfangreiche theoretische und praktische Wissensgrundlagen zum Aufbau und der Funktionsweise der Blockchain.
- Ein Blockchain-Entscheidungsmodell, um potenzielle Anwendungsfälle auf ihre Relevanz für den Einsatz von Blockchain zu prüfen.
- Ein Mehrwertindikationsmodell für Blockchain, zur Ermittlung der Aspekte des qualitativen Mehrwertes im Kontext Ihres konkreten Anwendungsfalls.
- Ein Ausblick über potenzielle Szenarien zur zukünftigen Weiterentwicklung dieser Technologie und ihren Auswirkungen auf unsere heutige Welt.

Im Übrigen haben Sie die Möglichkeit, die in diesem Buch vorgestellten Modelle als PDF unter dem nachfolgenden Link herunterzuladen: https://www.springer.com/de/book/9783658298210

Abschließend danke ich der IBM Deutschland, die mich bei der Ausarbeitung der Master-Thesis und somit während der initialen Entwicklung der nachfolgenden Modelle tatkräftig unterstützt hat.

Ich wünsche Ihnen viel Spaß beim Lesen sowie viele lehrreiche und gewinnbringende Erkenntnisse. Bei Fragen, Anmerkungen oder für sonstiges Feedback stehe ich Ihnen gerne jederzeit zur Verfügung und freue mich über Ihre Zuschriften.

Sie erreichen mich unter nicklas-urban@gmx.de.

P.S. Auf ein kleines, persönliches Highlight im Buch möchte ich Sie abschließend noch aufmerksam machen. Im gesamten Werk wird kein einziges

Mal das Wort *muss* oder eine davon abgeleitete Form verwendet. Sinnhaft spiegelt sich darin meine Lebenseinstellung wider – wir können alles unternehmen und erreichen, doch können vollkommen selbstständig entscheiden was wir angehen. Es gibt niemanden, der uns etwas aufzwingen kann.

Mai 2020 Nicklas T. Urban

Inhaltsverzeichnis

Abkürzungsverzeichnis

BTC	Bitcoin
DAC	Distributed Autonomous Corporation (verteiltes autonomes Unternehmen)
DAO	Distributed Autonomous Organization (verteilte autonome Organisationen)
Dapps	Distributed Applications (verteilte Anwendung)
DAS	Distributed Autonomous Society (verteilte autonome Gesellschaft)
DLA	Distributed Ledger Applikation (verteilte Anwendung)
DLT	Distributed Ledger Technologie
DT	Digital Twin (digitaler Zwilling)
EU	Europäische Union
GKV	Gesetzliche Krankenversicherung
IoT	Internet of Things (Internet der Dinge)
IT	Informationstechnologie
KI	Künstliche Intelligenz
KYC	Know Your Customer (Legitimationsprüfung)
PKV	Private Krankenversicherung
SLC	Smart Legal Contracts
TCE	Transaction Costs Economics
TTP	Trusted Third Party
WWW	World Wide Web
ZVS	Zentrale Vertrauensstelle

Einleitung 1

1.1 Motivation

Die Digitalisierung ganzer Wertschöpfungsketten prägt die derzeitige vierte industrielle Revolution, wobei sich etablierte Geschäftsmodelle, das bisherige Kundenverständnis sowie Kommunikationsprozesse und Netzwerke wandeln [1]. Mit Einführung des Internets hat sich der Informationsfluss bereits maßgeblich verändert *(Internet der Informationen).* Informationen können schneller und in größeren Mengen verarbeitet und übermittelt werden. Blockchain, eines der Trendthemen im Rahmen der Digitalisierung, verändert in diesem Zusammenhang den Austausch von materiellen, als auch immateriellen Werten *(Internet der Werte)* [2].

Blockchain ist erstmals als die Basistechnologie der Kryptowährung Bitcoin Ende 2008 bekannt geworden. Mit Bitcoin wurde ein fundamental neuer Weg geschaffen, Transaktionen online und digital abzubilden. Zentrale Organisationen wie Banken oder Broker werden nicht mehr benötigt [3]. Seitdem ist das öffentliche Interesse am Bitcoin sowie an Blockchain als Technologie stark gewachsen. Seit Start der Kryptowährung ist der Wert eines Bitcoins um das 20-Millionenfache gestiegen [4] und hat im Dezember 2017 einen Rekordwert von über 16.000 €/Bitcoin erreicht [5]. Das Trendthema Blockchain beschäftigt nicht mehr ausschließlich die Finanzindustrie, sondern stößt inzwischen in allen Wirtschaftszweigen auf großes Interesse. Damit gehen vielfältige Diskussionen über mögliche Einsatzszenarien, Potenziale sowie Auswirkungen einher. Viele Unternehmen beabsichtigen, die Blockchain-Technologie auch in das eigene Geschäftsumfeld zu integrieren. Gartner erwartet bis zum Jahr 2021 weltweite Investitionen von 38 Mrd. US$ in diese Technologie [6].

Doch der häufig hervorgehobene Hype klingt langsam ab und es entwickelt sich ein zunehmend klares Bild über konkrete Umsetzungsvorhaben und

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_1

produktive Anwendungen. Insbesondere im Finanzdienstleistungssektor, der Logistikindustrie und bei verarbeitenden Industrieunternehmen werden große Chancen gesehen. Die Adaption der Technologie durch diverse Geschäftsbereiche weitet das Spektrum der Anwendungsfälle aus. Hierbei zeichnet sich eine zunehmend komplexe Technologie-Landschaft ab, die von unterschiedlichen Blockchain-Frameworks, komplexen Integrationen mit bestehenden Systemen sowie der Sicherung der Netzwerke und Daten geprägt ist.

Währenddessen gewinnt Blockchain stark an strategischer Bedeutung. Neben Wirtschaftsunternehmen erkennen inzwischen primär politische Organisationen die Blockchain als wichtigen Wettbewerbsfaktor für die eigene Nation. Die europäische Union (EU) hat im Februar 2018 eigens eine Blockchain-Beobachtungsstelle und ein Blockchain-Forum gegründet [7]. Die EU möchte „aktiv dazu beitragen, dass Europa die neuen Chancen dieser Technologie nutzen kann, dass Expertenwissen aufgebaut wird und dass eine führende Rolle in diesem Bereich übernommen werden kann. Ziel ist es, Informationen zu sammeln, Trends zu beobachten und zu analysieren, Herausforderungen anzugehen und das sozioökonomische Potenzial dieser neuen Technologie auszuloten." [7] Neben der EU sieht die Bundesregierung großes ökonomisches Potenzial in der Blockchain-Technologie. Zunächst war Blockchain ein wichtiges Zukunftsthema im Koalitionsvertrag von 2018 [8] und wird von der 2019 veröffentlichten Blockchain-Strategie der Bundesregierung weiter unterstützt. Das Strategiepapier fokussiert das Schaffen konkreter regulatorischer Rahmenbedingungen, um Vermögenswerte in Zukunft digital abbildbar zu gestalten. Ziel der Bundesregierung ist es, die Grundlage für eine nachhaltigere Wirtschaft und einen fairen Wettbewerb am Innovationsstandort Deutschland zu schaffen [9].

Der Gartner Hype Cycle beschreibt Blockchain bereits als eine Technologie, die den Hype-Status überschritten hat und sich als Basistechnologie etabliert. Das Plateau of Productivity soll nach Gartner in den nächsten 2–5 Jahren (Stand 2019) erreicht sein. Des Weiteren bezeichnet Gartner die Blockchain-Technologie als derart vielfältig, dass Gartner hierfür einen eigenen Hype Cycle entwickelt hat, der einzelne Technologie-Bestandteile und Anwendungsgebiete in ihrer Evolution abbildet [10].

1.2 Zielstellung des Buches

Dieses Buch fokussiert die Blockchain-Technologie als eines der gegenwärtigen Trendthemen in der Digitalisierung. Daraus werden Potenziale und generierbare Mehrwerte für Geschäftsnetzwerke abgeleitet sowie anhand konkreter

Anwendungsbeispiele erläutert. Vielen Entscheidern ist Blockchain bereits ein Begriff, dem gegenwärtig ein hohes Potenzial zugeschrieben wird. Doch oft ist nicht eindeutig, in welchen Anwendungsfällen diese Technologie faktisch zielführend anwendbar ist. Hierzu beleuchtet dieses Buch entscheidende Kernelemente, die den Prozess von der ersten Anwendungsidee, über die Konzeption bis zur Umsetzungsplanung unterstützen.

Bei der Auswahl geeigneter Anwendungsfälle existieren derzeit große Unsicherheitsfaktoren und zahlreiche Unklarheiten. Laut einer Studie von Deloitte liegt die Überlebensrate von Blockchain-Projekten bei nur rund 8 %, wobei hier kommerzielle und nicht kommerzielle Pilotprojekte betrachtet wurden. Für ein Überleben im Sinne der Studie ist die aktive Wartung des Projektes Voraussetzung [11]. Viele Unternehmen befassen sich mit der Thematik Blockchain und investieren in diverse Projekte. Sie betrachten die Technologie gegenwärtig teils als Hype oder wichtige Innovation. Ein konkreter Mehrwert durch den Einsatz der Blockchain wird jedoch oftmals vernachlässigt. Dieser Effekt wird als Bandwagon-, auch Mitläufer-Effekt, bezeichnet. Er beschreibt eine gesteigerte Nachfrage nach einem Gut aufgrund der Tatsache, dass das Gut von anderen Personen konsumiert wird, nicht jedoch, weil die betreffende Person ein spezifisches Bedürfnis dafür hat [12].

Diesem Effekt wird in Kap. 3 begegnet, indem aufgezeigt wird, für welche Anwendungsfälle sich Blockchain tatsächlich eignet und welche Kriterien einen zielführenden Anwendungsfall beschreiben. Nicht jedoch soll das Interesse an der Technologie gemindert werden. Zentrale Fragestellung ist die folgende:

1. Welche Kriterien sollten für einen erfolgreichen Blockchain-Anwendungsfall berücksichtigt werden?
Zur Beantwortung dieser Frage wird ein Blockchain-Entscheidungsmodell entwickelt, mit dem potenzielle Anwendungsfälle auf ihre Relevanz für den Einsatz der Blockchain untersucht werden können. Ziel ist es, dass Anwendungsfälle umgesetzt werden, weil sich Blockchain für die konkrete Idee tatsächlich eignet und nicht, weil andere Organisationen mit Blockchain arbeiten oder die Technologie als Trend erachten.

Die Auffassungen zum Mehrwert von Blockchain sind stark differenziert. Einerseits gehen Experten davon aus, dass Blockchain das Potenzial besitzt, die Funktionsweise heutiger Wirtschaftssysteme vollständig zu revolutionieren. Andererseits stellen Experten Blockchain gleichzeitig als Hype dar, welcher nach einiger Zeit wieder obsolet wird [13, 14]. Nach Herausforderungen in der Skalierung der Blockchain-Netzwerke sowie fehlender rechtlicher Regulierungen, ist der unspezifische Mehrwert dieser Technologie dritthäufigster

Grund, digitale Projekte nicht auf Basis einer Blockchain umzusetzen [15]. Aus dieser Herausforderung leitet sich die zweite zentrale Fragestellung dieses Buches ab:

2. Inwiefern kann der Mehrwert von Blockchain für die Netzwerkteilnehmer qualitativ beschrieben werden?
Ziel soll es sein, qualitative Mehrwertaspekte der Blockchain, in Abhängigkeit zu einem konkreten Anwendungsfall, herauszustellen (Kap. 4). Es wird aufgezeigt, weshalb der Einsatz von Blockchain für ein konkretes Szenario durchaus zweckmäßig ist. Das Ergebnis soll folgend dazu dienen, weitere potenzielle Netzwerkteilnehmer vom Einsatz der Blockchain zu überzeugen. Hierfür wird ein Modell zur Identifizierung und Bewertung konkreter Mehrwertaspekte vorgestellt und anhand exemplarischer Anwendungsfälle erläutert.

Gegenwärtig wird Blockchain fokussiert in der Finanz- sowie Logistikbranche pilotiert, währenddessen die Auswirkungen der Technologie auf bestehende Geschäftsbeziehungen, Geschäftsmodelle und Systeme unterschiedlich dargestellt werden. Weiterhin beherbergen die bereits im *Gartner Hype Cycle for Blockchain Technologies* aufgeführten Komponenten und Anwendungsgebiete unterschiedliche Veränderungspotenziale. Hieraus ergibt sich die dritte zentrale Fragestellung:

3. Welche potenziellen Auswirkungen kann Blockchain auf bestehende Geschäftsmodelle und sozioökonomische Netzwerke haben?
Zur Konkretisierung der potenziellen Auswirkungen der Blockchain beschreibt Kap. 5 drei Evolutionsstufen dieser Technologie in Verbindung mit möglichen Anwendungsfällen sowie gegenwärtig bereits existierenden Pilotprojekten.

1.3 Gliederung und Aufbau des Buches

Zur Beantwortung der zuvor definierten zentralen Fragestellungen, gibt Kap. 2 zunächst einen Überblick zur Blockchain-Technologie (siehe Abschn. 2.1 und 2.2) und grenzt diese zur klassischen IT ab (Abschn. 2.3). Dieser Überblick dient als Grundverständnis zur Erörterung möglicher Einsatzbereiche sowie dem Verständnis für mögliche Auswirkungen und Potenziale.

Zum Einstieg in die Evaluierung möglicher Anwendungsfälle für den Einsatz der Blockchain-Technologie untersucht Kap. 3 zunächst bestehende Frameworks zur Evaluierung (Abschn. 3.1). Anschließend wird im Hinblick auf die erste

zentrale Fragestellung ein Entscheidungsmodell entwickelt (Abschn. 3.2 und 3.3), welches Defizite bestehender Ansätze behebt und dem Anwender zur Entscheidungsfindung dienen soll.

In Kap. 4 wird der qualitative Mehrwert der Blockchain-Technologie für Geschäftsnetzwerke untersucht (zweite zentrale Fragestellung). Zunächst identifiziert eine ausführliche Literaturanalyse bekannte Mehrwerte (Abschn. 4.2). Nachfolgend wird ein Modell zur Ermittlung des qualitativen Mehrwertes für ein konkretes Anwendungsszenario entwickelt (Abschn. 4.3 und 4.4).

Kap. 5 beschäftigt sich schließlich mit der dritten zentralen Fragestellung nach möglichen Auswirkungen auf heutige Ökosysteme und Geschäftsmodelle. Die drei Stufen von der Blockchain 1.0 bis hin zur Blockchain 3.0 werden anhand konkreter Fallbeispiele erläutert.

Der letzte Abschnitt (Kap. 6) fasst die Ergebnisse des Buches hinsichtlich der drei zentralen Fragestellungen zusammen und reflektiert die Ergebnisse der Arbeit.

1.4 Wie Blockchain gegenwärtigen Kernherausforderungen begegnet

Das Internet, auch als World Wide Web (WWW) bezeichnet, ist seit Anfang der 1990er Jahre kommerziell verfügbar. In der Zwischenzeit hat es sich als Grundlage der Informationsgesellschaft etabliert. Der Zugang ist nahezu kostenfrei, Informationen können zumeist frei eingesehen, als auch ohne großen Aufwand weltweit verbreitet werden. Es ist Grundlage für die heutige globale Vernetzung von Menschen und Organisationen. Währenddessen gilt Blockchain als Grundlage für die Wertegesellschaft und wird auch als *Internet der Werte* bezeichnet. Im Kern beschreibt die Blockchain-Technologie, die Idee eines verteilten, unveränderbaren Datenregisters und Netzwerkes, in dem Transaktionen chronologisch und transparent gespeichert sind. Diese *verteilte Transaktionsdatenbank* bildet eine Kette aus Datenblöcken, die jeweils mit dem chronologischen Vorgänger und dem chronologischen Nachfolger verknüpft sind und in Summe eine digitale Liste bilden, die die Werte ihrer Benutzer sowie die entsprechenden Transaktionen zu jedem Zeitpunkt dokumentiert. Im Vergleich zu herkömmlichen Datenbanken ist die Blockchain nicht auf einem einzelnen Server, sondern verteilt über das gesamte Netzwerk gespeichert. Jeder Netzwerkteilnehmer bzw. Server (auch als Node bezeichnet) verfügt über eine lokale Kopie der Blockkette. Jede Transaktion innerhalb des Netzwerkes wird direkt zwischen den Teilnehmern ohne vermittelnde Zwischeninstanz durchgeführt. Das Aussparen

zentraler, vertrauensbildender Intermediäre verändert die Machtverhältnisse innerhalb des Ökosystems und führt zumeist gleichzeitig zu Zeit- und Kostenersparnissen. Auswirken wird sich dies insbesondere auf Wirtschaftszweige, in denen Vertrauen essenziell ist und daher viele Intermediäre in heutige Prozesse eingebunden sind. Die Blockchain bildet das Transaktionsregister fälschungssicher und ohne die Einbindung zentraler Instanzen wie Zentralbanken, Zentralregister, Grundbuchämter und Notare ab (Details zur Funktionsweise der Blockchain-Technologie sind Abschn. 2.2 zu entnehmen).

Doch welche der gegenwärtigen Kernherausforderungen in der Wirtschaft und Gesellschaft begegnet Blockchain mit diesen Eigenschaften?
Zu Beginn dieses Buches und vor dem Einstieg in die Details der Technologie und geschäftlichen Komponenten, beleuchtet dieser Abschnitt eine Auswahl viel diskutierter gegenwärtiger Herausforderungen, in denen Blockchain zu Veränderungen führen kann. Die nachfolgenden, exemplarischen Herausforderungen sollen als Motivation für das Thema dienen und die potenziell weitreichenden Auswirkungen der Blockchain skizieren.

Herausforderung: Global Player Das digitale Zeitalter hat viele Veränderungen sowie neue Möglichkeiten für jeden einzelnen geschaffen. In Summe profitieren jedoch primär einige wenige globale Player, die große Plattformen geschaffen und deren Daten gezielt monetarisiert haben. Das Ergebnis ist eine Asymmetrie der Machtverhältnisse zwischen globalen Konzernen, Regierungen und einzelnen, natürlichen Personen [16].

Die Wirtschaftszeitschrift Fortune veröffentlicht jährlich eine Liste der 500 umsatzstärksten Unternehmen der Welt (Fortune Global 500). 2018 erwirtschaften diese Unternehmen zusammen einen Umsatz von rund 30 Billionen US$, [17] was in etwa 30–40 % der gesamten Weltwirtschaftsleistung entspricht. Gleichzeitig hat sich alleine seit Beginn des Internetzeitalters Anfang der 1990er Jahre bis 2019 die Weltwirtschaftsleistung vervierfacht [18]. Im Kern bedeutet dies, dass neue Technologien neue Möglichkeiten schaffen und die Wirtschaftsleistung stark fördern, sich die Steuerung dieser jedoch zunehmend zentralisiert.

Mit Blockchain als Internet der Werte könnte diese Verteilung der Macht von globalen Playern zurück an die einzelnen, natürlichen Personen gehen, indem der Werteaustausch (wie bspw. der Austausch von Besitzverhältnissen, Geldern oder Rechten) Peer-to-Peer möglich ist und weder für die Transaktion selbst, noch für die Aufbewahrung dieser, eine zentrale Instanz benötigt wird. Das Vertrauen wird mithilfe der digitalen Geschäftslogik innerhalb des Blockchain gebildet und bedarf keiner organisatorischen Instanz mehr.

Herausforderung: Korruption und Ungleichheit Korruption, Betrug und Intransparenz sind nicht nur ein politisch relevantes Thema, sondern laut der Global Shapers Survey des Weltwirtschaftsforums auch die weltweit führende Ursache für soziale Ungleichheit innerhalb von Ländern. Auch wenn Korruption in Entwicklungs- und Schwellenländern ein deutlich höheres Ranking erfährt, als in Europa oder Nordamerika, kommt insgesamt der Wunsch nach einer gleichberechtigten Gesellschaft hervor. In den Industriestaaten sind Einkommensunterschiede und Diskriminierung die Hauptursachen für Ungleichheit zwischen den Menschen [19].

Im Kern fehlt es an Transparenz innerhalb von Transaktionen und Handelsvereinbarungen, die Korruption begünstigen. Auch in diesem Aspekt kann Blockchain als transparentes, geteiltes Transaktionsregister zum Einsatz kommen. Gleichzeitig ist die vollständige Verifikation sowie Nachvollziehbarkeit aller Transaktionen und Besitzverhältnisse sichergestellt. Vereinbarte Regeln und Rechte werden zusätzlich fortlaufend geprüft. Die Ungleichheit aufgrund der asymmetrischen Einkommensverteilung sowie des Wachstums der *Schere zwischen Arm und Reich* lassen sich hingegen wiederum auf die Asymmetrien der Machtverhältnisse in der Weltwirtschaft zurückführen. Werden diese auf die einzelnen, natürlichen Personen umverteilt, könnten sich die Ungleichheiten in den Einkommen wiederum wandeln.

Herausforderung: Qualifiziertes Personal finden und Fachkräftemangel Der technologische Wandel erfordert neue Qualifikationen und Kompetenzprofile der Mitarbeiter in Unternehmen. Diese sehen sich zunehmend der Herausforderung gegenübergestellt, die richtigen sowie ausreichend Mitarbeiter am Arbeitsmarkt zu finden. Der Wirtschafts- und Finanznachrichtensender CNBC hat dies als eine der Top Herausforderungen für Unternehmen im Jahr 2019 geranked [20]. Doch sind es nicht ausschließlich IT-Fachkräfte oder hochqualifizierte Mitarbeiter die am Arbeitsmarkt knapp sind, oftmals sind primär in Industriestaaten auch viele Stellen im Sozialbereich (z. B. Pflege), dem Handwerk oder der Verwaltung unbesetzt [21].

Können keine (geeigneten) Mitarbeiter gefunden werden, gilt es, die Arbeit und Nachfrage der Kunden mit dem vorhandenen Personal zu beantworten. Da die Arbeitsleistung der Mitarbeiter und deren Output direkt mit der Arbeitszeit korreliert und nur begrenzt skalierbar ist, nimmt die Automatisierung von Vorgängen einen immer höheren Stellenwert ein. Mit dem Aufkommen der Informationstechnologie (IT) wurden bereits viele, einfache Prozesse automatisiert. Die verstärkte Entwicklung künstlicher Intelligenz (KI) bzw. fortgeschrittener Entscheidungsalgorithmen ermöglicht zunehmend die automatisierte

Abbildung komplexerer Vorgänge. Limitiert ist dies jedoch maßgeblich durch die Qualität sowie das Vorhandensein einer geeigneten Datengrundlage. Blockchain als ein Netzwerk zwischen allen Organisationen innerhalb eines Wertschöpfungsnetzwerkes sowie vertrauensvolles Transaktionsregister, kann die erforderliche Datenbasis für die zukünftige, weitere Automatisierung und Digitalisierung von Geschäftsprozessen und Geschäftsmodellen erbringen (siehe auch Abschn. 5.3).

Herausforderung: Kommunikationsgeflecht und Kundenservice Zuletzt zahlt die Automatisierung der Geschäftsvorgänge zusätzlich auf den Kundenservice ein. Kunden erwarten zunehmend digitale Prozesse, eine sofortige Bearbeitung und Beantwortung ihrer Anliegen oder Wünsche. Manuelle Prüfschritte können entfallen, indem Transaktionen innerhalb der Blockchain immer automatisch validiert werden. Weiterhin werden Medien- und Systembrüche, die ggf. manuelle Schnittstellen bedingen, vermieden. Befinden sich alle Teilnehmer eines Geschäftsökosystems im selben Netzwerk, ist die Kommunikation mit allen Partnern über nur eine digitale Schnittstelle möglich. Individuelle Datenaustauschverfahren, die eine manuelle Informationsübermittlung oder papiergebundene Prozesse bedingen, können gänzlich entfallen. Das komplexe, globale Kommunikationsgeflecht kann somit auf einfache Weise neu definiert und genutzt werden. Dem Endkunden werden schnellere und digitale Angebote ermöglicht (siehe auch Abschn. 5.1).

Zusammenfassend kann Blockchain der Grundbaustein und gleichzeitig Schlüssel für eine fairere und gerechtere Gesellschaft werden, in der Daten, Rechte sowie die Finanzverwaltung zum Allgemeingut der Gesellschaft werden. Die Technologie kann jedem Menschen, insbesondere auch in weniger entwickelten Ländern, einen sicheren und vertrauensvollen Zugang zu globalen Märkten und Netzwerken schaffen.

Literatur

1. Geissbauer, R./Koch, V./Kuge, S./Schrauf, S. (2014). *Chancen und Herausforderungen der vierten industriellen Revolution.* o. O.: PwC.
2. IBM. (2016). *Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View*. Rockledge: IBM.
3. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* o. O.: o. V.
4. Sixt, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie.* Wien: Springer Gabler.
5. BTC-ECHO. (2020). *Bitcoin-Kurs*. Abgerufen am 20.02.2020 von BTC-ECHO – Bitcoin & Blockchain Pioneers: https://www.btc-echo.de/kurs/bitcoin/

6. Kaletovic, D. (15. Juni 2018). *Banks Spent $1.7B On Blockchain Last Year*. Abgerufen am 03.08.2019 von Nasdaq: https://www.nasdaq.com/articles/banks-spent-17b-blockchain-last-year-2018-06-15
7. Europäische Kommission. (2018). *Europäische Kommission bringt EU-Blockchain-Beobachtungsstelle und -Forum auf den Weg.* Brüssel: Europäische Kommission.
8. Bundesregierung. (2018). *Koalitionsvertrag - Ein neuer Aufbruch für Europa, Eine neue Dynamik für Deutschland, Ein neuer Zusammenhalt für unser Land.* Berlin: Bundesregierung.
9. BMWi/BMF. (2019). *Blockchain-Strategie der Bundesregierung: Wir stellen die Weichen für die Token-Ökonomie.* O. O.: BMWi/BMF.
10. Gartner. (12. September 2019). Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years. Abgerufen am 10.10.2019 von Gartner: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows
11. Fromhart, S./Srinivas, V./Trujillo, J. (2017). *Evolution of blockchain technology.* o. O.: Deloitte.
12. Piekenbrock, D. (19. Februar 2018). *Mitläufereffekt*. Abgerufen am 23.10.2019 von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/mitlaeufereffekt-37630/version-261064
13. Buchter, H./Nienhaus, L. (06. Dezember 2017). *Genie und Wahnsinn*. Zeit Online.
14. Schwarz, M. (31. Okotober 2017). *Blockchain-Technologie – Hype oder digitaler Mehrwert?* Abgerufen am 16.11.2019 von KMA-Online: https://www.kma-online.de/aktuelles/it-digital-health/detail/hype-oder-digitaler-mehrwert-a-36036
15. McLellan, C. (02. Dezember 2019). *Blockchain and business: Looking beyond the hype*. Abgerufen am 12.12.2019 von ZDnet: https://www.zdnet.com/article/blockchain-and-business-looking-beyond-the-hype/
16. McKinsey. (2016). How blockchains could change the world. Abgerufen am 14.09.2019 von McKinsey: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world
17. Fortune. (2019). Global 500. Abgerufen am 14.09.2019 Fortune: https://fortune.com/global500/2019/
18. The World Bank (2019). *GDP (current US$).* Abgerufen am 14.09.2019 von The World Bank: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD
19. World Economic Forum. (2017). *Global Shapers Survey 2017*. o. O.: World Economic Forum.
20. Mitchell, C./Odland, S. (29. Januar 2019). *Survey: CEOs are worried about 3 things this year – and No. 1 is whether you plan to quit.* Abgerufen am 14.09.2019 von CNBC: https://www.cnbc.com/2019/01/28/the-3-biggest-challenges-facing-ceos-in-2019-and-how-to-solve-them.html
21. Statista. (2019). *Statistiken zum Fachkräftemangel*. Abgerufen am 25.11.2019 von Statista: https://de.statista.com/themen/887/fachkraeftemangel

Blockchain als verteilte Netzwerktechnologie

2

Die Identifizierung geeigneter Blockchain-Anwendungsfälle sowie möglicher Potenziale setzt ein Grundverständnis der Basis-Technologie voraus. Insbesondere gilt es zu verstehen, was sich auf Basis der Blockchain umsetzen lässt, was jedoch nicht. Hierzu gibt dieses Kapitel zunächst einen Überblick über die Entwicklungshistorie (Abschn. 2.1). Außerdem werden die technischen Grundlagen und die Funktionsweise der Blockchain dargestellt sowie Unterschiede zwischen einzelnen Blockchain-Implementierungen aufgezeigt (Abschn. 2.2). Zuletzt erfolgt eine Gegenüberstellung der Blockchain-Technologie mit herkömmlichen Systemen sowie dem klassischen IT-Verständnis (Abschn. 2.3).

2.1 Entwicklungshistorie

Das Interesse an der Blockchain-Technologie, insbesondere im Kontext von geschäftlichen Anwendungen, ist gegenwärtig immens. Zunächst hat die auf Blockchain basierende Kryptowährung *Bitcoin,* als ein möglicher Blockchain-Anwendungsfall, mit starken Wertsteigerungen großes öffentliches Interesse in allen Medien hervorgerufen. In der Zwischenzeit hat sich der anfängliche Hype zunehmend gelegt, das Interesse für mögliche Anwendungen in vielen Branchen ist dafür stark gestiegen.

Der Weg zur Blockchain Technologisch betrachtet ist Blockchain selbst allerdings nicht neu. Aus technischer Sicht reichen die Wurzeln von Blockchain in das Jahr 1980 zurück. Damals verglich Ralph Merkle in seinem Paper *Protocols For Public Key Cryptosystems* verschiedene digitale

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_2

Kryptographie-Lösungen miteinander und fokussierte sich primär auf die Verteilung von öffentlichen Schlüsseln sowie digitaler Signaturen innerhalb eines Netzwerkes. In diesem Zusammenhang sind die *Merkle-Trees* entstanden [1], die später für die Umsetzung von Bitcoin genutzt werden. Ebenfalls Berücksichtigung in der Umsetzung des Bitcoins findet die Arbeit von Haber und Storneta aus dem Jahre 1991 [2]. In ihrem Paper *How to time-stamp a digital document* stellen sie einen Lösungsansatz für das Setzen eines digitalen Zeitstempels auf Daten mittels ihrer Methode *Linked Timestamping* (verkettete Zeitstempel) vor. Hintergrund ihrer Arbeit ist der Schutz von geistigem Eigentum. Ziel sollte es sein, digitale, leicht modifizierbare Medien zu schützen und parallel zu zertifizieren, wann ein Dokument erstellt bzw. zuletzt geändert wurde. Die Daten sollten nachträglich weder in die Vergangenheit, noch in die Zukunft gelegt werden können. Der Kern des Problems bestand darin, die Daten zeitlich zu stempeln, nicht nur das Medium. Dazu haben sie auf mathematische Verfahren zur digitalen Zeitstempelung der Daten zurückgegriffen, wobei die Privatsphäre des Dokuments gewahrt wird, indem kein externer Dienst, wie ein Zeitstempeldienst, eingebunden wird [3]. In der heutigen Blockchain-Logik finden sich zudem *Smart Contracts* wieder, die 1997 von Nick Szabo erstmals erwähnt wurden. Er beschreibt Smart Contracts als „a set of promises, specified in digital form, including protocols within which the parties perform on these promises." [4] Dabei ermöglichen Computer im Rahmen der Digitalisierung das Ausführen von Algorithmen bzw. Regelwerken, welche bisher aufwändig und entsprechend teuer waren. Diese Algorithmen bilden die Bedingungen realer Verträge in digitaler Form ab und überwachen somit permanent die Einhaltung dieser, wenn eine Vertragspartei im Netzwerk Transaktionen ausführt. Szabo hat die digitale Abbildung (in Form von Algorithmen) von Verträgen bewusst als *smart* bezeichnet, da er die *neuen* Verträge als flexibler und funktionaler einordnet, als die bisherige Form auf Papier, zumal Smart Contracts ihre Einhaltung im Netzwerk selbst kontrollieren können. Zusätzlich sind Smart Contracts als Programmcode eindeutig verständlich, wohingegen Papierverträge in natürlicher Sprache verfasst und damit nicht zwangsläufig eindeutig interpretierbar sind. Die Nutzung künstlicher Intelligenz hat Szabo bewusst ausgeklammert, vielmehr sollen die bisher auf Papier festgehaltenen Vertragsklauseln als asynchrones Protokoll in die Hard- und Software eingebettet werden und zwischen den Parteien implementiert sein [4].

Neben Lösungsansätzen zur Sicherung geistigen Eigentums unter Nutzung von Zeitstempeln auf Datenebene, hat Stefan Konst 2000 eine allgemeine Theorie zur kryptografisch abgesicherten Verkettung von Daten vorgestellt. In seiner

Arbeit stellt er Lösungsansätze vor, wie die Authentizität, Reihenfolge und Vollständigkeit der Einträge einer Log-Datei sichergestellt werden kann, wobei die Log-Datei um weitere Einträge erweiterbar sein soll. Dazu hat er kryptografische Verfahren angewandt, welche Ecken eines Graphen über die Bildung von Kanten miteinander verketten [5]. Als letzte Vorarbeit für die Blockchain-Technologie kann, wenn auch später nicht mehr erwähnt, das Paper *Distributing trust on the Internet* von Christian Cachin betrachtet werden. In seinem Paper beschreibt er die Architektur für eine sichere und fehlertolerante Replikation in einem asynchronen, verteilten Netzwerk wie dem Internet, in dem gezielte Hackerangriffe Server schädigen und das Netzwerk kontrollieren könnten. Er stellt neue, allgemeine Fehlermuster mit entsprechenden Protokollen vor, welche eine realistische Darstellung von Vertrauensannahmen über (gewichtete) Schwellenmodelle modellieren [6].

Bitcoin als erste Blockchain Kurz nach der Finanzkrise 2008, veröffentlichte ein anonymer Autor unter dem Pseudonym Satoshi Nakamoto ein Forschungspapier, in dem eine reine Peer-to-Peer-Anwendung für Online-Zahlungen, Bitcoin genannt, vorgestellt wurde. Geld kann direkt von einem Nutzer an einen anderen übermittelt werden, ohne ein Finanzinstitut zu durchlaufen. Digitale Signaturen stellen einen entscheidenden Teil der Lösung dar, welche den Wegfall einer vertrauenswürdigen dritten Partei, bisher ein Finanzinstitut, ermöglicht [2]. Bitcoin, als die populärste Kryptowährung, die von keinem Staat und keiner Bank kontrolliert wird und international grenzenlos gehandelt werden kann, verbreitet sich verstärkt. Im Dezember 2017 erreicht Bitcoin den historischen Spitzenwert von über 16.000 €/BTC [7]. Zum Vergleich, beim Start der Kryptowährung im Oktober 2009 konnte ein Bitcoin für 0,0008 US$ erworben werden und entsprach damals den ungefähren Strom- und Hardwarekosten für das Mining. Im Juli 2010 wurde Bitcoin erstmals über die Bitcoin-Börse Mt. Gox zu einem Kurs von 0,06 US$ pro Bitcoin gehandelt [8].

Die Architektur dieser Netzwerkstruktur sorgt gleichzeitig dafür, dass *Double-Spending* verhindert wird [2]. Unter Double-Spending versteht man in der Finanzwelt die Problematik, dass insbesondere bei digitalen Überweisungen keine Gelder doppelt ausgegeben werden dürfen [9]. Bitcoin löst das Problem innerhalb des Peer-to-Peer-Netzwerkes, indem ein Zeitstempel zusammen mit den Transaktionsdaten (inklusive einem Link zum vorherigen Datenblock) gehasht und somit eine fortlaufende Sequenz als Kette erstellt wird, welche im Nachhinein nicht mehr verändert werden kann [2].

Definition

Ein Hashwert bezeichnet einen alphanumerischen Wert fester Länge, der durch eine Hashfunktion erzeugt wird. Hashfunktionen basieren auf mathematischen Verfahren, die aus beliebigen Daten Hashwerte festgelegter Länge erzeugen, wobei eine kleine Änderung der Ausgangsdaten zu vollständig verschiedenen Hashwerten führt. Der Hashwert selbst erlaubt keine Rückschlüsse auf die Ausgangsdaten und lässt sich grundsätzlich mit sehr geringem Rechenaufwand berechnen. ◀

Zielsetzung von Bitcoin ist es, eine transparente, verteilte Finanznetzwerkplattform zu schaffen, die anonym bleibt und keine zentrale Vertrauensstelle (ZVS) braucht [2]. Details zur Funktionsweise von Blockchain, siehe Abschn. 2.2.

Von Blockchain selbst sprach Nakamoto zu diesem Zeitpunkt noch nicht. Dieser Begriff entwickelte sich erst im Laufe der Zeit aus seiner Funktion heraus, da die einzelnen Transaktionen zusammen mit dem Zeitstempel und dem Hash als Datenblock gespeichert und über die einzelnen Hashwerte miteinander verkettet werden. Im Ergebnis eine Kette aus Datenblöcken, im Englischen als Blockchain bezeichnet [10].

Neben Bitcoin wurde 2013 das Projekt der Ethereum-Blockchain vorgestellt, wozu Gavin Wood 2014 die technische Spezifikation herausgebracht hat. Ethereum stellt zum einen die Basis für die Kryptowährung Ether [11], ist heute aber auch eine der wichtigen Blockchain-Plattformen für viele individuelle Anwendungen, die auf dieser technologischen Grundlage frei gestaltet werden können, wobei Kryptowährungen nur einen möglichen Anwendungsfall für die Blockchain-Technologie darstellen. Damit unterscheidet sich Ethereum im Wesentlichen von der Bitcoin-Blockchain, auf der keine selbstentwickelten Anwendungen neben Bitcoin als Kryptowährung betrieben werden können.

Als erste Branche sahen vorrangig Finanzdienstleister ihre Geschäftsmodelle durch Blockchain bedroht und haben frühzeitig den Anstoß für die Entwicklung privater Blockchains gegeben, um die neue Technologie perspektivisch für eigene Finanztransaktionen nutzen zu können [12]. Mit Start des Hyperledger Projekts durch die Linux Foundation im Dezember 2015, ist die private, permissioned Blockchain (Erläuterung siehe Abschn. 2.2), auch als *Blockchain for Business* bezeichnet, als interessante Plattform für viele geschäftliche Anwendungsfälle entstanden. IBM und Intel sind als zwei wesentliche Partner aktiv an diesem Projekt beteiligt und entwickeln die *Hyperledger Fabric* bzw. *Hyperledger Sawtooth* Blockchain auf Basis von Open Source und Open Governance Standards [13]. Im geschäftlichen Bereich setzt sich parallel die Grundidee durch, Blockchain vermehrt zur Gewährleistung von technisch erzeugtem

Vertrauen zwischen beliebigen Parteien innerhalb eines geschäftlichen Netzwerkes bzw. verschiedenen Partnern, die an einem Geschäftsvorgang beteiligt sind, zu nutzen. Neben dem Hyperledger Projekt haben sich zwischenzeitlich viele neue Blockchain-Frameworks gebildet. Eines der verbreiteteren ist Corda. Corda ist 2016 erstmals vorgestellt worden und hat zu Beginn den Fokus der Anwendungsbereiche primär auf die Finanz- und Versicherungsbranche gelegt [14]. Die Entwicklung erfolgt durch R3, ein Zusammenschluss von gegenwärtig (Stand Herbst 2019) über 300 Partnern aus Wirtschaft und Forschung [15].

2.2 Technische Grundlagen der Blockchain

Wie im vorherigen Kapitel dargelegt, sind Kryptowährungen nur einer von vielen möglichen Anwendungsfällen der Blockchain-Technologie und Bitcoin stellt lediglich eine technische Implementierung dar. Blockchain wird auch als „general purpose technology“ [16] verstanden, die gleichzeitig transparent, flexibel und effizient eine verteilte Datenhaltung und Konsensfindung ermöglicht [16]. Um ein einheitliches Verständnis zu schaffen, wird Blockchain nachfolgend definiert und die technischen Grundlagen sowie Unterschiede zwischen verschiedenen Implementierungen erläutert.

Definition

Die Distributed Ledger Technologie (DLT) beschreibt einen Ansatz für die verteilte Dokumentation von Transaktionen. Gegenüber dem klassischen Ansatz, das Ledger (zu Deutsch Hauptbuch) von einer zentralen Instanz zu verwalten, wird das Hauptbuch mittels DLT dezentral über beliebig viele gleichgestellte Parteien organisiert, die jeweils eine gleichberechtigte Kopie des Ledgers besitzen. Parallel ist sicherzustellen, dass neue Transaktionen in allen lokalen Kopien übernommen werden und ein gemeinsamer Konsens bzgl. des aktuellen Status des Ledgers gefunden wird.

Für die technische Umsetzung stellt Blockchain eine adäquate Technologie dar, die in der Lage ist, genau diese Anforderungen zweifelsfrei sicherzustellen. Blockchain ermöglicht das verteilte Speichern von Datenregistern, ohne eine vertrauenswürdige Drittpartei einzubinden, wie sie bspw. Banken bei Finanztransaktionen darstellen. Jede Partei im Netzwerk verfügt über eine eigene lokale Kopie der Transaktionshistorie und kann Transaktionen verifizieren. Zusätzlich wird der Konsens mit Hilfe der Smart Contracts und Konsensalgorithmen automatisch sichergestellt. ◀

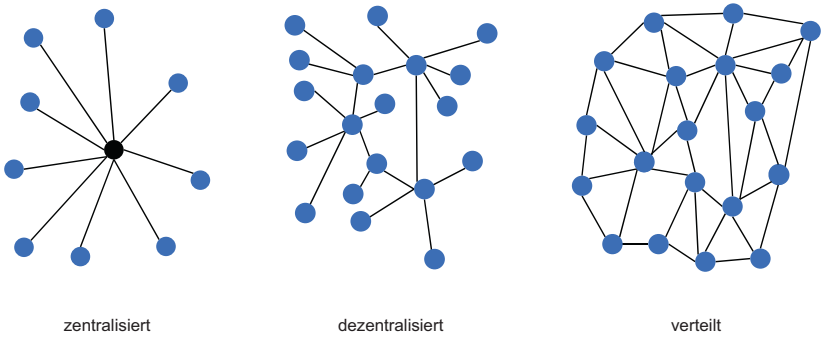

Abb. 2.1 Gegenüberstellung zentraler, dezentraler und verteilter Systeme. (Eigene Darstellung)

Die bisher zentrale Datenspeicherung, Transaktionsprüfung und Autorisierung übernimmt das Blockchain-Netzwerk. Im Gegensatz zu zentralen (bspw. das Telefonnetz in den Anfängen) und dezentralen Systemen (bspw. das Internet) ist bei verteilten Systemen jeder Netzwerknoten direkt in das Netzwerk integriert und kann von dort mit allen anderen Knoten interagieren (Abb. 2.1). Eine zentrale Stelle, die alle Kommunikationswege bündelt oder einzelne Verteilerknoten, welche Teilbereiche des Netzwerkes bündeln, gibt es nicht. Diese Architektur schützt das Netzwerk zudem vor Ausfällen und Cyberangriffen, indem der Ausfall einzelner Knotenpunkte das Netzwerk nicht zum Erliegen bringt sowie ein Angreifer für eine erfolgreiche Datenmanipulation gezwungen wäre, mehr als 50 % der Netzwerkknoten zur gleichen Zeit in gleicher Weise zu verändern [17].

Ein Blockchain-Netzwerk beinhaltet mehrere Knoten (jeder Knoten kann vereinfacht als kleiner Server betrachtet werden), welche die im Netzwerk durchgeführten Transaktionen sowohl validieren, als auch speichern. Dabei besitzt jeder teilnehmende Knoten eine eigene lokale Kopie der gesamten Blockchain (auch als Shared Ledger bezeichnet), somit eine Auflistung aller jemals im Netzwerk durchgeführten Transaktionen [18]. Wird eine neue Transaktion im Netzwerk angestoßen, wird diese im Netzwerk verteilt und das Resultat der Transaktion von allen validierenden Knoten berechnet, bspw. der Wert von Variablen nach Durchführung der Transaktion. Die einzelnen Knoten melden die Resultate im Netzwerk zurück, woraufhin mit Hilfe von Konsens-Algorithmen die Übereinstimmung, der gemeinsame Konsens, bestimmt werden kann. Gleichzeitig wird die Integrität im geteilten Netzwerk sichergestellt. Wird eine vorab definierte Akzeptanz unter den Knoten erzielt, d. h. eine kollektive Zustimmung der Knoten zur jeweiligen Transaktion erreicht (bspw. 80 % Übereinstimmung

der Ergebnisse), gilt die Transaktion als freigegeben und wird durchgeführt. Die Transaktion wird als weiterer Block in vorgegebener Reihenfolge in den lokalen Blockchain-Kopien angehangen (Abb. 2.2). Der Prozess zur Konsensbildung sowie zur Erstellung und Verteilung eines neuen Blocks ist abhängig vom Konsens-Mechanismus und der konkreten Blockchain-Implementierung [19]. Ein Beispiel ist der Proof-of-Work Algorithmus, der u. a. im Bitcoin oder Ethereum Netzwerk eingesetzt ist, jedoch viel Rechenleistung erfordert. Für die Berechnung eines neuen Blocks mit dem Proof-of-Work Algorithmus gilt es, aus den Transaktionen, dem Hashwert des vorherigen Blocks sowie einer Zufallszahl (auch als Nonce bezeichnet) einen Hashwert zu berechnen, der eine definierte Anzahl führender Nullen aufweist. Der Berechnungsprozess (auch als Mining Prozess bezeichnet) besteht somit im Kern aus dem Testen einer Vielzahl verschiedener Zufallszahlen, um einen passenden Block-Hash zu erreichen. Je mehr Rechenleistung ein einzelner Miner im Netzwerk besitzt, desto mehr Rechenoperationen kann dieser pro Sekunde durchführen, wodurch wiederum die Wahrscheinlichkeit steigt, der Erste zu sein, der den neuen Block errechnet hat und vom Netzwerk entlohnt wird. Ziel dieses Verfahrens ist die Verteilung der Validierung der Transkationen und Berechnung der neuen Blöcke im Netzwerk, um eine zentrale Instanz zu umgehen [2]. Der Proof-of-Stake Algorithmus hingegen verteilt die Berechnung eines neuen Blocks innerhalb der Blockchain über ein Zufallsprinzip, wodurch das rechenintensive Wettrennen um die Berechnung des neuen Blocks nicht benötigt wird. Daneben existieren noch einige weitere Algorithmen, insbesondere im Zusammenhang mit permissioned Blockchain-Implementierungen, die jedoch nicht Teil dieses Buchs sein sollen.

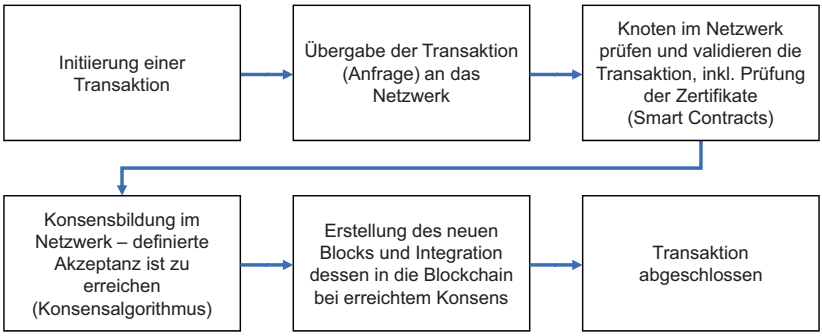

Abb. 2.2 Ablauf einer Transaktion innerhalb einer Blockchain – schematisch. (Eigene Darstellung in Anlehnung an Prinz, 2017, S. 18)

Die Vorgehensweise, die Daten verteilt vorzuhalten, sorgt für zusätzliches Vertrauen innerhalb des Netzwerkes, da jeder Teilnehmer eine eigene lokale Datenkopie hält und demzufolge nicht mehr auf die Richtigkeit der Daten auf Servern anderer vertrauen braucht. Bei Systemen mit zentraler Datenhaltung haben bisher alle Teilnehmer darauf vertraut, dass der Besitzer und Administrator der Datenbank deren Inhalte nicht verändert. Mit Hilfe des Shared Ledgers können zusätzlich einmal durchgeführte Transaktionen, bedingt durch die Verkettung der Blöcke, im Nachgang weder verändert noch manipuliert werden. Jede Änderung in den Daten würde zu einem neuen Hashwert des jeweiligen Blocks führen und damit die Verlinkung zum vorherigen Block aufheben (Abb. 2.3). Eine Veränderung einer Transaktion würde zudem nur die lokale Kopie der Blockchain auf einem Knoten verändern. Für einen wirksamen Angriff bzw. Manipulation der Daten, gilt es einen Großteil (>50 %) der lokalen Kopien auf den Knoten innerhalb des Blockchain-Netzwerkes gleichzeitig in gleicher Weise zu verändern. Währenddessen wächst die Blockkette jedoch stetig weiter, indem neue Transaktionen als neue Blöcke fortlaufend angefügt werden.

Definition

Der Begriff der Transaktion unterscheidet sich je nach Blockchain-Implementierung und konkretem Anwendungsfall. Im Fall von Finanzanwendungen kann eine Überweisung als eine Transaktion fungieren. Dies gilt auch für den Transfer von Bitcoins von einer Bitcoin-Adresse (digitales Konto im Bitcoin-Netzwerk) zu einer anderen Bitcoin-Adresse.

Im Bereich von Blockchain-basierten Lieferketten kann eine Transaktion die Erstellung des digitalen Zwillings (englisch Digital Twin, kurz DT) eines physischen Produktes darstellen sowie eine weitere Transaktion den DT von einem Besitzer zu einem anderen transferieren. Die Aktualisierung des Status oder weiteren Variablen des DT sind ebenfalls als Transaktion zu verstehen.

Grundsätzlich bezeichnet eine Blockchain-Transaktion somit einen konkreten Vorgang innerhalb des Netzwerkes, welcher als Funktion im Smart Contract definiert sowie dort mit entsprechenden Regeln hinterlegt ist. ◀

Tab. 2.1 veranschaulicht die Veränderung der Hashwerte bei Veränderung nur einer Ziffer im Datensatz. Das Ergebnis ist ein vollkommen verschiedener Hashwert, der zudem keine Rückschlüsse auf die Ausgangsdaten zulässt (Basis: SHA 1 Algorithmus). Diese Hashwerte dienen innerhalb der Blockchain als Verlinkung der einzelnen Blöcke (Abb. 2.3).

Da einmal in der Blockchain gespeicherte Transaktionen nicht mehr gelöscht werden können, lassen sich Transaktionen allenfalls mittels einer neuen Transaktion,

Tab. 2.1 Exemplarische Veränderung des Hashwertes bei geringfügiger Anpassung des Datensatzes

Nutzer-ID	Attribut 1	Attribut 2	Hashwert (SHA 1)
J45851236	grau	63	9382921a794df64b26e61bea26bdf3a4c32f4cf6
J45851237	grau	63	7dce1dbcc7bd9ea79b5eadf214640a9eff7048f9

im Rahmen einer Rückbuchung, korrigieren. Vergleichbar ist dieses Verfahren mit einer Korrekturbuchung in der betriebswirtschaftlichen Buchführung.

Neben dem Vertrauen stellen die lokalen Kopien der Blockchain den gemeinsamen Konsens im Netzwerk sicher, da alle Teilnehmer jederzeit[1] den vollständigen und exakt gleichen Datenbestand zur Verfügung haben. Ferner gibt es keinen Single Point of Trust, keine zentrale Vertrauensstelle, der alle Teilnehmer in dem Netzwerk bzw. Ökosystem vertrauen brauchen [20].

Struktur und Aufbau der Blockchain Wie dem Namen Blockchain zu entnehmen ist, handelt es sich um eine Verkettung von Blöcken, die zum Speichern von Transaktionsdaten dient [19]. Dabei ist jeder Block mittels eines kryptografischen Hashwertes mit dem jeweils vorherigen verbunden. Der Block als eigentliche Datenstruktur beinhaltet neben der Verlinkung zum vorherigen Block, die gespeicherten Transaktionen (Datensätze) sowie die entsprechenden Zeitstempel (Abb. 2.3) und die jeweilige digitale Signatur der Teilnehmer. Der

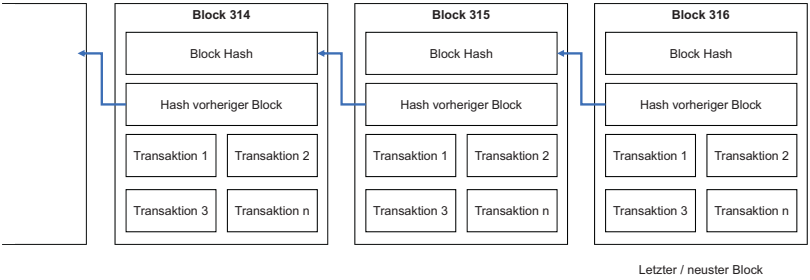

Abb. 2.3 Struktur der Blockchain. (Eigene Darstellung in Anlehnung an Nakamoto 2008, S. 3)

[1]Korrekt betrachtet besteht im Netzwerk eine Karenzzeit von bis zu wenigen Sekunden, in der unterschiedliche Datenstände bei den Teilnehmern existieren. Diese Zeit entsteht aufgrund der architekturbedingten technischen Kommunikationsverzögerung (Errechnen und verteilen der Blöcke im Netzwerk).

Hashwert eines Blockes errechnet sich wiederum aus dem Hashwert des vorherigen Blockes (Verlinkung), den Inhalten der Transaktionen, den Zeitstempeln und ggf. weiterer vereinbarter Variablen (beim Bitcoin bspw. die Zufallszahl). Wird versucht in einem bestehenden Block eine Transaktion nachträglich zu manipulieren, so ändert sich im Zuge dessen zwangsläufig der Hashwert dieses Blocks. Die Verlinkung zum nachfolgenden Block ist damit nicht mehr gegeben, da dort weiterhin der ursprüngliche Hashwert enthalten bleibt [21].

Zusammenfassend wird das Vertrauen in der Blockchain durch die verteilte Datenspeicherung auf verschiedenen Knotenpunkten in Verbindung mit der Verlinkung der einzelnen Blöcke erreicht, welches eine Manipulation durch eine zentrale Instanz ausschließt. Eine Veränderung der Daten[2] würde unweigerlich zu einer Unterbrechung der Kette führen, eine Manipulation wäre sofort nachweisbar [20].

Im Kern lässt sich die Grundidee der Blockchain mit fünf fundamentalen Eigenschaften beschreiben:

- *Unveränderbarkeit:* Sobald die Transaktion der Blockchain hinzugefügt wurde, ist sie unveränderbar gespeichert.
- *Nicht-Abstreitbarkeit:* Da alle historischen Transaktionen kryptografisch signiert und nachvollziehbar sind, ist eine revisionssichere Überprüfbarkeit der gespeicherten Daten möglich.
- *Integrität:* Die Blockchain bietet Datenintegrität bezüglich der Richtigkeit und Konsistenz der gespeicherten Daten mittels kryptografischer Verfahren.
- *Transparenz:* Alle Netzwerk-Teilnehmer haben öffentlichen Zugriff auf die Blockchain und die darin gespeicherten Daten, wodurch die volle Transparenz sichergestellt ist.
- *Gleiche Rechte:* Jeder Knoten (Teilnehmer) im Netzwerk hat die gleichen Zugriffs- und Schreibrechte innerhalb der Blockchain [22]

Gegenwärtig existieren bereits verschiedene Blockchain-Implementierungen, die diese grundlegenden Eigenschaften der Blockchain aus Effizienz, Performance und geschäftlichen Gründen verschieden auslegen und umsetzen. Insbesondere die vollständige Transparenz sowie die gleichen Rechte im Netzwerk sind in

[2]Wenn, ließen sich die Daten nur auf direkter Speicherebene auf dem Laufwerk manipulieren. Demzufolge betrifft ein Manipulationsversuch in diesem Zuge einen konkreten Peer (Netzwerkknoten) und nicht sofort das gesamte Netzwerk.

vielen geschäftlichen Anwendungen nicht gewünscht oder nicht praktikabel. Hier gilt es, einen Kompromiss aus Transparenz und Privatsphäre abzubilden, denn ein vollständig transparentes System würde es jedem Teilnehmer ermöglichen, alle Information einzusehen, eine Privatsphäre wird nicht gewährt. Hingegen unterbindet ein vollständig privates System jegliche Transparenz [21]. Zur Wahrung des persönlichen Datenschutzes innerhalb des Netzwerkes kann ein Shared Ledger die öffentliche Statusprüfung gemäß dem Verwendungszweck der Anwendung bereitstellen. Weitere Informationen über den Zustand des einzelnen Teilnehmers werden nicht offengelegt. Bspw. können Daten Off-Chain, d. h. außerhalb der Blockchain lokal bei jedem Teilnehmer gespeichert werden, wobei nur ein Hashwert dieses Datensatzes in der Blockchain geteilt wird. Der Hashwert ermöglicht die Verifizierbarkeit des ursprünglichen Datensatzes. Der spätere Empfänger eines Datensatzes kann selbst den Hashwert errechnen und diesen mit dem in der Blockchain hinterlegten Hashwert vergleichen. Sind beide Werte identisch, hat der Empfänger die Ursprungsdaten vom Sender erhalten. Ein weiterer möglicher Ansatz, die Privatsphäre zu wahren, stellt die Verwendung kryptografischer Verschlüsselungstechniken dar, wobei nur die Teilnehmer Daten einsehen können, denen gezielt der Schlüssel mitgeteilt wird [23]. Ein Anwendungsbeispiel für die Kompensation von Transparenz, Anonymität bzw. Privatsphäre und öffentlicher Nachvollziehbarkeit stellen e-Voting-Systeme (Systeme für digitale Abstimmungen) dar. Hierbei gilt es, die Anonymität jedes Nutzers zu wahren, während zeitgleich die volle Transparenz sowie die öffentliche Nachvollziehbarkeit gewährleistet sein sollen, um Manipulationsversuche sowie eine Doppelabstimmung (Analog zum Double-Spending Problem) zu unterbinden [21].

Permissionless und permissioned Blockchain-Implementierungen Aufgrund dieser Überlegungen sind zusätzlich zu den ursprünglichen permissionless (nicht zugangsbeschränkte) Blockchain-Implementierungen, wie z. B. Bitcoin, auch permissioned (zugangsbeschränkte) Blockchains, wie z. B. das Hyperledger Projekt entstanden. Bei einer permissionless Blockchain kann jeder Teilnehmer dem Netzwerk zu jedem beliebigen Zeitpunkt beitreten oder es wieder verlassen, es existiert keine Instanz, welche die Mitglieder verwaltet bzw. einzelne Teilnehmer vom Netzwerk ausschließen kann. Diese Offenheit impliziert, dass jeder Teilnehmer zunächst den gesamten Inhalt der Blockchain einsehen und aktiv als schreibende Partei agieren kann, d. h. alle Arten der Transaktion ausführen und sich unmittelbar an der Konsensfindung, bei Bitcoin z. B. dem Mining-Prozess

[2], beteiligen kann. Auch hier sind kryptografische Ansätze möglich, durch welche der Leserkreis einzelner Inhalte wiederum beschränkt werden kann, um einen bestimmten Grad an Privatsphäre umzusetzen [21].

Bei einer permissioned Blockchain hingegen werden zu Beginn alle Teilnehmer durch eine gemeinsame Einheit autorisiert und ihnen definierte Rollen und Rechte zugewiesen. Hierbei ist eine gezielte Unterscheidung zwischen Lese- und Schreibrechten für einzelne Datensätze möglich. Es kann definiert werden, ob alle Teilnehmer Zugriff auf alle Transaktionen haben (public permissioned Blockchain) oder Leserechte zwischen den Teilnehmern explizit unterschieden werden sollen (private permissioned Blockchain) [24]. Weiterhin können permissioned Blockchains durchaus simplere und effizientere Konsens- und Validierungsalgorithmen ermöglichen, da das (Grund-)Vertrauen in der zugriffbeschränkten Implementierung durch die Autorisierung und Registrierung aller Teilnehmer zu Beginn erfolgt. In der permissionless Blockchain wird dieses Vertrauen ausschließlich über die Konsens- und Validierungsalgorithmen sichergestellt [25]. Die bekanntesten Implementierungen der permissioned Blockchain stellen Hyperledger Fabric und Corda dar. Um die Sicherheit weiter zu erhöhen, ist es möglich, verschiedene Parteien in separaten, miteinander verbundenen Blockchains (interconnected) agieren zu lassen. Konkret können permissionless und permissioned Blockchains über definierte Schnittstellen (Konnektoren) miteinander verbunden werden. In Bezug auf einen Geschäftsvorgang wird bspw. ein definiertes, öffentliches Datenset, mit der permissionless Blockchain geteilt, wohingegen private Datenanhänge nur in der permissioned Blockchain gespeichert werden. Beide Datensets sowie Transaktionen stehen über den Konnektor in Verbindung. Die Unveränderbarkeit wird gleichzeitig mittels Hashwerten sichergestellt. Die Kombination einer permissionless und einer permissioned Blockchain zu einer ganzheitlichen Lösung wird auch als Hybrid-Blockchain bezeichnet [21, 26, 27].

Rollen und Funktionen in der Netzwerkarchitektur Je nach Definition kann in einem Netzwerk ergänzend zu lesenden und schreibenden Teilnehmern auch in validierende und regulierende Parteien unterschieden werden. Bei regulierenden Parteien handelt es sich im weiteren Sinne um lesende Teilnehmer, die im Rahmen von bestimmten Gesetzen oder Regelungen die erfolgten Transaktionen nachvollziehen und nachprüfen. Bspw. kann für Zwecke der Wirtschaftsprüfung eine Prüfinstanz als Netzwerknoten eingebunden werden, die erfolgte Transaktionen mitliest und separat vom Netzwerk prüft, d. h. unabhängig von den Smart Contracts. Validierende Parteien hingegen lassen sich von schreibenden Parteien insofern abgrenzen, dass die schreibenden Parteien Transaktionen

anstoßen (Transaktionen als Anfrage in das Netzwerk stellen) und diese an das Netzwerk zur Konsensfindung übergeben, nicht jedoch zwangsläufig die Smart Contracts ausführen und die neuen Blöcke errechnen. Die validierenden Teilnehmer übernehmen hierzu die Ausführung der Smart Contracts und somit die Prüfung der Transaktionsanfragen, ohne jedoch selbst Transaktionsanfragen in das Netzwerk zu übersenden [21]. Im Sinne der Bitcoin Blockchain werden validierende Parteien als Miner bezeichnet [2]. Weiterhin unterscheiden einige Quellen technisch zwischen aktiven und passiven Netzwerkteilnehmern. Aktive Netzwerkteilnehmer sind Organisationen, die selbst einen eigenen Netzwerknoten betreiben. Passive Teilnehmer hingegen nutzen den Zugang zur Blockchain über einen aktiven Teilnehmer, betreiben jedoch selbst keinen physischen Netzwerkknoten [28]. Ein Beispiel für passive Netzwerkteilnehmer sind Kunden eines Einzelhändlers, die mittels einer Kunden-App des Händlers Produktbarcodes scannen und deren Lieferkette über die Blockchain abfragen und nachvollziehen können.

Auch wenn diese Art der Rollenverteilung durchaus an die Administration herkömmlicher zentraler Systeme erinnert, besteht hierbei ein entscheidender Unterschied: Bei einer zentralen Datenbank war bisher jeder Nutzer gezwungen, dem ihm zur Verfügung gestellten Datenbestand zu vertrauen, es war ihm jedoch nicht möglich, die Echtheit sowie Richtigkeit der Daten zu verifizieren. Anders bei der Nutzung einer Blockchain: Zwar kann je nach Implementierung auch hier durchaus nicht jeder Nutzer alle Dateninhalte einsehen, doch besteht für jeden Nutzer die Möglichkeit, jederzeit den Status des Ledgers infolge der Verkettung anhand der Hashwerte zu überprüfen. Auch ohne Einsicht aller Daten genügt die Prüfung der Hashwerte der einzelnen Blöcke, um Manipulationen nachweisen zu können [21].

Smart Contracts Wie in Abschn. 2.1 bereits angeführt, bilden Smart Contracts eine wichtige Grundlage für die heutigen Blockchain-Implementierungen. Sie können als autonome Programme betrachtet werden, welche in die Blockchain-Implementierung eingebunden sind und definierte Geschäftsregeln als Programmcode darstellen. Durch ihre Integration lassen sich auch komplexe Regelwerke digital abbilden und ihre Bedingungen automatisch prüfen, sobald ein Smart Contract durch die Anfrage von bestimmten Transaktionen ausgeführt wird [29]. Auch, wenn der Begriff Smart Contract den Anschein eines Vertrages weckt, stellt dieser selbst (d. h. der Quellcode) keinen rechtsverbindlichen Vertrag dar, sondern ist ein Stück Programmcode, der einen zwischen den Parteien vereinbarten rechtlichen Vertrag widerspiegeln kann [19].

Davon abzugrenzen sind *Smart Legal Contracts* (SLC), die tatsächlich rechtskräftige Verträge darstellen, welche über *Distributed Ledger Applikationen* (DLA), wie z. B. Blockchain, zwischen den teilnehmenden Parteien geschlossen werden [30]. Auf Grundlage von Smart Legal Contracts lassen sich sogenannte *dezentralisierte autonome Organisationen* (DAO) entwickeln. Eine moderne Organisation ließe sich somit ausschließlich durch entsprechende Verträge mit ihren Managern, Mitarbeitern, Lieferanten sowie Kunden definieren. Sollten alle Verträge im Sinne der SLC automatisiert sein, ist es durchaus denkbar, eine solche Organisation gänzlich ohne menschliche Interaktion zu führen. Diese Organisation könnte, inkl. dem dazugehörigen Ökosystem, dementsprechend autark agieren [31]. Vertiefende Informationen zur Nutzung der Smart Legal Contracts in Verbindung mit DAOs befinden sich im Kap. 5.

Orakel Eine zusätzliche Automatisierung innerhalb eines Blockchain-Netzwerkes kann durch Orakel[3] erreicht werden, indem diese dem Netzwerk eine Schnittstelle zu externen Systemen oder Datenbanken bieten. Mittels der Orakel lassen sich sowohl Daten aus dem Blockchain-Netzwerk in andere Systeme speichern, als auch im Zuge bestimmter Transaktionen Daten aus anderen, externen Quellen abrufen. Bspw. ließen sich Echtzeitpreise von Produkten abfragen und einer Verkaufstransaktion beifügen. Auch eignen sich Orakel durchaus zum externen Speichern großer Datenmengen. Zwar wird bei Blockchain die maximale Speichergröße innerhalb eines Blocks von der konkreten technischen Implementierung definiert, aufgrund der Architektur ist es jedoch wenig zielführend, große Datenmengen, wie bspw. Sensordaten, direkt in einer Blockchain zu speichern. Diese könnten in externen Datenbanken gespeichert werden, wobei das Orakel lediglich einen Hashwert als Link und Manipulationssicherung in die Blockchain überführt [32].

Neben Orakeln als Verbindung zu externen Datenquellen, führen Blockchain-Implementierungen wie bspw. Hyperledger Fabric eine interne Zustandsdatenbank (als World State bezeichnet) je Netzwerkknoten. Die Zustandsdatenbank bildet den gegenwärtigen Netzwerkstatus ab. Werden einzelne Stati infolge einer Transaktion geändert, bleibt nur der letzte Stand in der Datenbank gespeichert. Übertragen auf Finanztransaktionen entspricht der Zustand dem aktuellen Kontostand jedes Kontos. Ziel dieser Datenbank ist die effiziente

[3]Orakel ist als Bezeichnung für die technische Schnittstelle zu verstehen und ist nicht zu verwechseln mit dem amerikanischen Soft- und Hardwarehersteller Oracle Corp.

Abfrage aktueller Variablen sowie das Starten von Transaktionen, ohne zuvor jedes Mal die Kette von Blöcken von Beginn an durchzurechnen. Letzteres ist jedoch möglich, um die Richtigkeit der Daten in der Zustandsdatenbank zu verifizieren [33].

Zusammenfassend ist festzuhalten, dass das größte Potenzial der Blockchain in der Bildung und Sicherstellung von Vertrauen und Transparenz, insbesondere in digitalen Ökosystemen, liegt. Erreicht wird dies vorrangig durch die nicht manipulierbare bzw. unveränderbare Datenspeicherung bei parallel automatisierter Prüfung aller Transaktionen durch den Einsatz von Smart Contracts. Experten erhoffen sich durch diese Technologie die vollständige Abschaffung von Mittelsmännern oder Drittparteien, die Transaktionen oft aufwändiger und ineffizienter machen.

2.3 Abgrenzung von traditioneller und disruptiver IT

Die traditionelle Informationstechnologie fokussiert sich primär auf die Digitalisierung bisheriger Prozesse, meist verbunden mit der Zielvorgabe, diese effizienter zu gestalten. Bei traditionellen IT-Projekten steht oft das Ziel im Vordergrund, papierbasierte oder manuelle Prozessabläufe digital und automatisiert abzubilden. Häufig werden bestehende Prozessschritte nur in eine digitale Form überführt, die Organisationen und Abläufe im Hintergrund bleiben jedoch größtenteils unberührt (dort setzt das Process Re-Design an). Das nachfolgende Beispiel verdeutlicht hierbei den Unterschied zwischen inkrementell-evolutionären Neuerungen (auf Basis traditioneller IT) und radikal-revolutionären Innovationen (auf Basis disruptiver IT).

Beispiel

Der Papierscheck als Zahlungsmittel, der händisch ausgefüllt und unterschrieben wurde, ist mittels PIN-gesicherter Kreditkarte ersetzt worden. Diese digitale Form arbeitet jedoch analog auf Grundlage ähnlicher Speicher- und Organisationsmodelle sowie dem vorhergehenden Prüfsystem. Gleiches gilt für Onlineüberweisungen, wobei die Eingabe und die Verarbeitung vollkommen digital erfolgen, jedoch das herkömmliche Papierformular einzig in eine digitale Eingabemaske mit annähernd denselben Prozessen im Hintergrund überführt wurde. Derartige Innovationen gehören zu den inkrementell-evolutionären Neuerungen, der „die kontinuierliche Verbesserung einzelner Produkt- oder Prozessparameter bei einer gleichzeitigen Beibehaltung des bestehenden Grundprinzips“ [34] zu Grunde liegt.

Dem gegenüber steht bspw. PayPal, die den Prozess der Geldüberweisung vollkommen neugestaltet haben (vgl. radikal-revolutionäre Innovation). Statt das herkömmliche Überweisungsformular in eine digitale Onlinemaske zu überführen, bei der die Überweisung noch immer mehrere Tage in Anspruch nimmt, kann mittels PayPal Geld innerhalb weniger Sekunden nur mit Angabe einer E-Mailadresse versendet werden. Dabei entstehen (zwischen Privatpersonen) weder Gebühren, noch brauchen lange Zahlenreihen eingegeben und verifiziert werden. Zusätzlich ist der Bezahldienst jederzeit online verfügbar. ◀

Blockchain als Technologie lässt sich als radikal-revolutionäre Innovation (auch disruptive IT) einstufen, die „mit der Anwendung neuer Wirkprinzipien oder der völligen Neugestaltung von Abläufen und Strukturen“ [34] einhergeht. Neben einem vollständig anderen Grad der Innovation, grenzt sich Blockchain von der traditionellen IT in ihrer Struktur und Rolle der Technologie ab. Tab. 2.2 zeigt die wesentlichen Unterscheidungsmerkmale beider Technologien auf, um ein Verständnis der revolutionären und disruptiven Eigenschaften der Blockchain-Technologie zu erhalten. Bei Betrachtung der Tabelle ist zu beachten, dass ggf. je nach Implementierung einzelne Merkmale abweichen können.

Tab. 2.2 Gegenüberstellung von Blockchain und traditioneller IT (vgl. Bhardwaj und Kaushik 2018, S. 266) und (vgl. Gervais und Wüst 2017, S. 3)

Attribut	Blockchain	Traditionelle IT/Datenbanken
Datenbesitz und Datenschutz	Verteilte Datenhaltung mit (meistens) einem Verschlüsselungsalgorithmus	Zentral gesteuert und überwacht; Datenschutz ist direkt abhängig von dem Datenbankadministrator
Datenspeicherung	Primär nur Speicherung der Transaktionen in verketteten Datenblöcken	Datenspeicherung primär in Tabellenform (Zeilen & Spalten)
Datenzugriff	Für permissionless Blockchains i. d. R. gleich für alle Netzwerkknoten, in permissioned Blockchains abhängig vom Rollen- und Rechtekonzept	Gesteuert durch zentrale Administration
Datengültigkeit & Überprüfbarkeit	Transparent, Datenvalidierung durch alle Netzwerkteilnehmer	Gezielte, einzelne Datenbankabfragen, ohne Validierung einzelner Datensätze bzw. Transaktionen

(Fortsetzung)

Tab. 2.2 (Fortsetzung)

Attribut	Blockchain	Traditionelle IT/Datenbanken
Transaktion	Mit allen Knoten geteilt und durch diese validiert	Zentrale Administration steuert und verwaltet alle Transaktionen
Sicherheit	Erhöhte Sicherheit, da jeder Block mit seinem Vorgänger verlinkt ist und nicht manipuliert werden kann; Zusätzlich gibt es keine zentrale Datenquelle die angegriffen werden könnte	Nicht besonders sicher, da Daten nicht validiert werden können und alle Daten zentral an einem Ort gespeichert sind
Zentral administriert	Nein	Ja
Öffentlich verifizierbar	Ja (bei permissioned Blockchain ggf. eingeschränkt)	Nein
Datenintegrität	Ja, Daten sind garantiert vor unautorisierter Bearbeitung geschützt	Nein
Transparenz	Abhängig von der Blockchain-Implementierung, typischerweise komplett transparent	Abhängig von den Sicherheitseinstellungen durch den zentralen Administrator, i. d. R. nicht gegeben
Robustheit	Verteiltes System – Angreifer greift jeden Knoten einzeln und parallel an	Zentrales System – ein zentraler Angriffspunkt

Abschließend ist anzumerken, dass sich mittels der Distributed Ledger Technologie nicht nur Prozesse digital abbilden lassen. Vielmehr werden die organisatorischen Ökosysteme, die Geschäftsmodelle beteiligter Parteien sowie die möglichen Services, die dem Endkunden angeboten werden können, von Grund auf neugestaltet. Gleichzeitig stellen genau diese Änderungen bzw. Möglichkeiten die größten Herausforderungen bei der Umsetzung von Blockchain-Projekten dar. Die organisatorische Skalierung von Pilotprojekten bildet zumeist die größte Herausforderung, da eine Einigung aller beteiligten Partner auf einen Standard in Bezug auf bspw. die Smart Contracts, die Validierungslogik sowie ein Datenmodell notwendig ist.

Literatur

1. Merkle, R. (1980). *Protocols for Public Key Cryptosystems*. *IEEE Symposium on Security and Privacy*, 122–134.
2. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* o. O.: o. V.
3. Haber, S./Stornetta, S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology, 3*(2), 99–111.
4. Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Abgerufen am 10.09.2019 von Phonetic Sciences: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
5. Konst, S. (2000). *Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge.* Braunschweig: TU Braunschweig.
6. Cachin, C. (2001). *Distributing Trust on the Internet*. Zürich: IBM.
7. BTC-ECHO. (2020). *Bitcoin-Kurs*. Abgerufen am 20.02.2020 von BTC-ECHO – Bitcoin & Blockchain Pioneers: https://www.btc-echo.de/kurs/bitcoin/
8. Sixt, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie.* Wien: Springer Gabler.
9. Giese, P./Kops, M./Preuss, M./Wagenknecht, S./de Boer, D. (2016). *Die Bitcoin Bibel Das Buch zur digitalen Währung.* Kleve: BTC-ECHO.
10. Cavus, M. (18. April 2016). *Blockchain – Wer hat's erfunden?* Abgerufen am 25.09.2019 von Digitale Excellenz: https://www.digitale-exzellenz.de/blockchain-wer-hats-erfunden/
11. Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger.* o. O.: o. V.
12. Gantner, T./Nack, D./Schwarz, M./Schwarz, R./Winkler, J. (2017). *Blockchain: Die Demokratisierung des Gesundheitswesens?* Leipzig: Wissenschaftliches Institut für Gesundheitsökonomie und Gesundheitssystemforschung.
13. The Linux Foundation. (2018). *About Hyperledger*. Abgerufen am 10. Juni 2018 von Hyperledger: https://www.hyperledger.org/about
14. Brown, R./Carlyle, J./Grigg, I./ Hearn, M. (2016). *Corda: An Introduction*. o. O.: o. V.
15. R3 (2019). Our story. Abgerufen am 25.11.2019 von R3: https://www.r3.com/history/
16. Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain.* o. O.: o. V.
17. Blockgeeks. (2018). *What is Blockchain Technology?* Abgerufen am 04. Juli 2018 von Blockgeeks: https://blockgeeks.com/guides/what-is-blockchain-technology/
18. Evans-Greenwood, P./Harper, I./Hillard, R./Williams, P. (2016). *Bitcoin, Blockchain, and Distributed Ledgers: Caught between promise and reality.* o. O.: Deloitte.
19. Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Staples, M., Tran, A., Zhu, J. (2017). *Risks and opportunities for systems using blockchain and smart contracts*. Sydney: Data61.
20. Morabito, V. (2017). *Business Innovation Through Blockchain.* Mailand: Springer.
21. Gervais, A./Wüst, K. (2017). *Do you need a Blockchain?* Zurich: ETH Zurich.
22. Xu, X./Weber, I./Staples, M./Zhu, L./Bosch, J./Bass, L./Rimba, P. (2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design.* Sydney: Data61.

23. Kunde, E., Kaulartz, M., Ben Naceur, M., Liban, S., Kunz, M., Skwarek, V., Liesenjohann, M. (2017). *Blockchain und Datenschutz – Faktenpapier.* Berlin: Bitkom.
24. Gupta, M. (2017). *Blockchain for dummies.* Hoboken: John Wiley & Sons, Inc.
25. Kadiyala, A. (18. Februar 2018). *Nuances Between Permissionless and Permissioned Blockchains*. Abgerufen am 14. Juni 2018 von Medium: https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483
26. Smilo. (2018). The latest generation hybrid blockchain platform. o. O.: Smilo.
27. The Institutes. (2017). *Blockchain Building Blocks: Creating a world of opportunity for insurance from an evolving area of technology*. Malvern: The Institutes.
28. Distributed Vision. (10. Februar 2017). *Introduction to Blockchain*. Abgerufen am 29.10.2019 von Distributed Vision Blog: http://www.distributed.vision/articles/blockchain-articles/introduction-to-blockchain
29. Clack, C., Bakshi, V., & Braine, L. (2016). *Smart Contract Templates: foundations, design landscape and research directions*. o. O.: Barclays Bank PLC.
30. Sandner, P./Valenta, M. (2017). *FSBC Working Paper – Comparison of Ethereum, Hyperledger Fabric and Corda.* Frankfurt am Main: Frankfurt School of Finance & Management.
31. Omohundro, S. (2014). Cryptocurrencies, Smart Contracts, and Artificial Intelligence. *AI Matters, 1*(2), 19–21.
32. Kakavand, H./Kost De Sevres, N. (2016). *The Blockchain Revolution: An Analysis of Regulation and Technology related to distributed Ledger Technologies*. o. O.: o. V.
33. McCallum, T. (10. Februar 2018). *Diving into Ethereum's world state*. Abgerufen am 19.10.2019 von Medium: https://medium.com/cybermiles/diving-into-ethereums-world-state-c893102030ed
34. Brem, A./Vahs, D. (2015). *Innovationsmanagement: Von der Idee zur erfolgreichen Vermarktung.* Stuttgart: Schäffer-Poeschel.
35. Bhardwaj, S., & Kaushik, M. (2018). Blockchain – Technology to Drive the Future. *Smart Computing and Informatics Proceedings of the First International Conference on SCI 2016, 78*, 263–271.

3 Erfolgreiche Blockchain-Anwendungsfälle identifizieren

Der Weg zum richtigen und zielführenden Blockchain-Anwendungsfall ist genau die Herausforderung, die letztendlich über den Erfolg einer neuen Anwendung entscheidet. Während zu beginn, in der Hochphase des Blockchain-Hypes, viele Unternehmen versucht haben, Blockchain für alle möglichen Anwendungsgebiete einzusetzen, hat sich das Bild inzwischen gewandelt. Unternehmen sind bedachter bei Start eines neuen Blockchain-Projekts. Die Fragen sind jedoch weiterhin dieselben: Eignet sich Blockchain für den konkreten Anwendungsfall? Und wenn ja, welche Art der Blockchain ist die richtige?

Dieses Kapitel fokussiert dazu die Evaluierung von potenziellen Anwendungsfällen und entwickelt dafür ein Blockchain-Entscheidungsmodell. Das Entscheidungsmodell ist nicht einzig für technisch orientierte Nutzer geeignet, sondern soll primär von Ansprechpartnern und Entscheidern aus den Fach- und Innovationsbereichen genutzt und verstanden werden. Für die Schrittweise Hinführung zum Modell, wird zunächst der gegenwärtige Stand der Technologie sowie der Anwendungsfälle zusammenfassend betrachtet und die Grundlage für das Entscheidungsmodell gelegt (Abschn. 3.1). Anschließend werden Kriterien extrahiert, die einen erfolgreichen und effizienten Anwendungsfall für die Blockchain-Technologie ausmachen (Abschn. 3.2). Auf Basis dieser Kriterien wird das Modell erstellt, indem die einzelnen Kriterien mittels eines Flussdiagramms gruppiert abgefragt werden (Abschn. 3.3). Abschließend wird ein übergreifendes Resümee gezogen (Abschn. 3.4).

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_3

3.1 Situation – Wo stehen wir heute?

Die Hype-Phase der Blockchain-Technologie ist mittlerweile überwunden, dennoch ist diese Technologie nach wie vor ein aktuelles Thema in den sozialen Geschäftsnetzwerken. Viele Technologieunternehmen vermarkten Blockchain zudem aktiv, wodurch sich Unternehmen aller Branchen dazu aufgefordert sehen, sich mit dieser Technologie auseinanderzusetzen und sie nach Möglichkeit in ihre bestehenden Geschäftsmodelle oder Angebote zu integrieren. In der Folge entstehen viele Ideen und Projekte zu diversen möglichen Anwendungen, welche jedoch nicht alle zwingend zielführend sind. Vielmehr werden oft Innovationsprojekte vorangetrieben, die die Blockchain-Technologie als Grundlage nehmen und nach einem geeigneten Anwendungsfall suchen. Dabei wird oftmals nicht das Business Problem in den Fokus gestellt und die am besten geeignete Technologie evaluiert, sondern Blockchain als gesetzte Lösung angesehen.

Ziel ist es, ein Modell bzw. Framework anzubieten, mit dem potenzielle Blockchain-Anwendungsfälle in Bezug auf ihre Relevanz für den Einsatz der Blockchain-Technologie analysiert werden können. Letztendlich soll dieses Modell neben der Evaluierung von potenziellen Anwendungsfällen für Blockchain folgende Fragen beantworten:

1. Ist Blockchain die geeignete Technologie für die Realisierung des spezifischen Anwendungsfalls?
2. Wenn ja, welche Art der Blockchain eignet sich am besten für die Realisierung?

Weiterhin ist die detaillierte Evaluierung möglicher Anwendungsfälle für Blockchain mit Fokus auf das umstrittene Potenzial sowie die Abgrenzung zu traditionellen Informationstechnologien sinnvoll. Zudem kann der Nutzen sowie der generierbare Mehrwert durch Blockchain in der geplanten Anwendung herausgestellt werden. Folglich eignet sich das Modell gleichermaßen dazu, für den spezifischen Anwendungsfall nachvollziehbar zu belegen, warum Blockchain bei der Implementierung den herkömmlichen Technologien überlegen ist und entsprechend vorgezogen werden sollte. Zur Evaluierung des qualitativen Mehrwertes einer Blockchain-Anwendung siehe jedoch Kap. 4.

3.2 Herausforderung – Wie finde ich den richtigen Anwendungsfall?

Analyse bestehender Blockchain-Entscheidungsmodelle Der Weg zum richtigen und zielführenden Anwendungsfall gestaltet sich meist als komplex. In der Literatur werden oftmals einige, wenige Kriterien für sinnvolle Blockchain-Anwendungsfälle genannt. Ein hinreichendes Modell oder Framework, mit dem Anwendungsfälle auf ihre Relevanz für den Einsatz der Blockchain-Technologie validiert werden können, existiert in dieser Form nicht. Zur Aufarbeitung relevanter Kriterien und Hinführung zu einem umfassenden Modell, werden nachfolgend drei Forschungsarbeiten dargestellt, die Teilbereiche eines möglichen Blockchain-Entscheidungsmodelles betrachten.

IBM, als eines der führenden Unternehmen in der Implementierung und Entwicklung der Blockchain-Technologie, stellt in seinem Founders Handbook für Blockchain vier wesentliche Kriterien für erfolgreiche Blockchain-Anwendungsfälle in den Fokus: (Hamilton et al. 2018, S. 9)

- Does the solution require trusted data to be shared across multiple parties without a central authority?
- Are assets being transferred between parties?
- Is there a need for privacy among participants in the current business network?
- Is there the need for greater trust inside the current business network?

Aus Sicht von IBM geben die Antworten auf diese vier Fragen im Kern Aufschluss darüber, in welchem Umfang ein potenzieller Anwendungsfall den möglichen Mehrwert der Technologie effizient nutzen würde und die Architektur einer Blockchain somit sinnvoll wäre. Generell adressieren diese Fragen den Kern der Blockchain: Vertrauen, Durchführung von Transaktionen ohne zentrale Vertrauensstelle sowie ein (Geschäfts-) Netzwerk mit mehreren Teilnehmern. Für die Auswertung der Antworten bleibt indessen jedoch immer ein Blockchain-Experte erforderlich. Eine Kategorisierung der Antworten oder ein Entscheidungsbaum wird nicht vorgestellt [1].

Wesley Graham, Consultancy Manager für Blockchain bei Berkeley, einer führenden studentischen Blockchain-Organisation in den USA, geht in seinem Entscheidungsmodell (siehe Abb. 3.1) hingegen bereits detaillierter und mit verstärktem Fokus auf den Einsatz beim Kunden vor. Mit seinem Entscheidungsbaum, welchen er selber als Checkliste beschreibt, möchte er besonders bedeutungsvolle Use Cases identifizieren. Sein Flussdiagramm fragt zunächst ab,

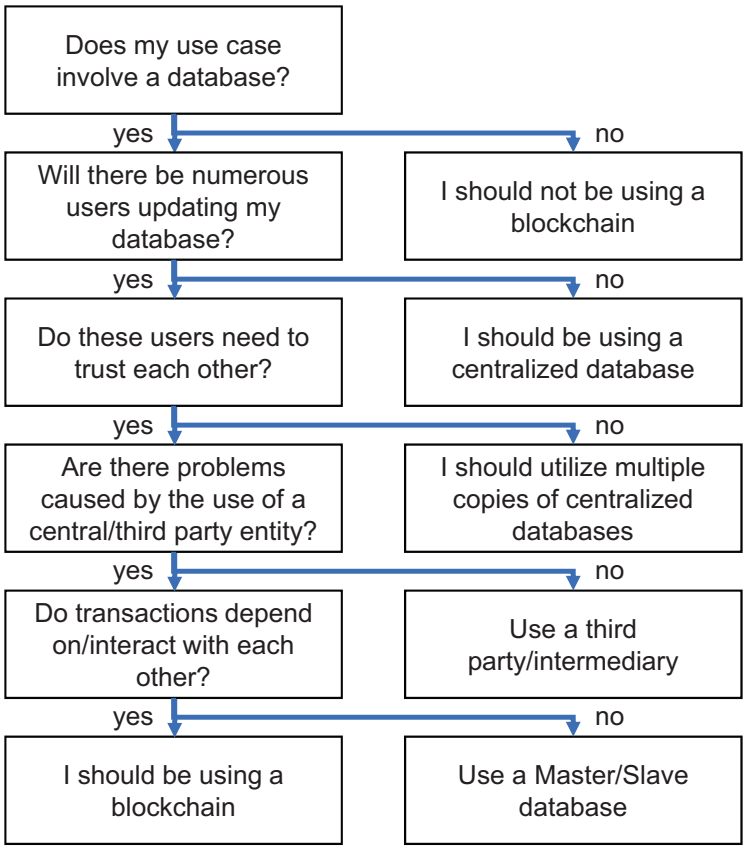

Abb. 3.1 Blockchain-Entscheidungsmodell nach Graham. (Eigene Darstellung in Anlehnung an Graham 2018, S. 3)

ob im geplanten Anwendungsfall Daten gespeichert und von mehreren Parteien aktualisiert werden sollen und hierzu eine gemeinsame Vertrauensbasis benötigt wird. Diese Fragestellungen dienen zur Unterscheidung zwischen einer zentralen und einer dezentralen Datenbank. Um die Blockchain-Relevanz weiter abzugrenzen, wird zusätzlich nach Problemen mit einer zentralen Vertrauensstelle sowie der Abhängigkeit zwischen den an einer Transaktion beteiligten Parteien gefragt. Können alle Fragen mit Ja beantwortet werden, ist der Anwendungsfall Grahams Modell zufolge für den Einsatz einer Blockchain geeignet. In seinem

Modell nimmt Graham eine detaillierte Unterscheidung zwischen zentralen, dezentralen sowie Master-Slave Datenbanken vor, lässt hingegen offen, welche Art der Blockchain für den spezifischen Anwendungsfall am empfehlenswertesten ist [2].

Graham schreibt jedoch ebenfalls:

> „[Blockchains] like Hyperledger [are] […] private enterprise blockchains designed to decentralize these transaction ecosystems, supporting the global business transactions of major technological, financial and supply chain companies. It is important to note that these implementations are exceptional – not ordinary" [2]

Das lässt darauf schließen, dass permissioned Blockchains aus seiner Sicht keine Verbreitung im Markt haben werden bzw. eher die Ausnahme darstellen und demzufolge in seinem Modell keine Berücksichtigung finden. Die gegenwärtige Situation, insbesondere im Enterprise-Bereich, zeigt jedoch eine gegenläufige Entwicklung.

Ebenfalls anhand eines Entscheidungsbaums (siehe Abb. 3.2) haben Gervais und Wüst untersucht, unter welchen Umständen ein bestimmtes Szenario mit der Blockchain-Technologie faktisch sinnvoll lösbar ist oder ob alternative Technologien, wie zum Beispiel ein zentrales Datenbanksystem, besser geeignet wären. Entgegen den zuvor aufgezeigten Modellen, unterscheiden sie bei ihrer Betrachtung allgemein zwischen permissionless und permissioned Blockchains. Für die Evaluierung von Anwendungsfällen definieren Wüst und Gervais einige grundlegende Fragen zur Notwendigkeit, Daten zu speichern, ob es mehrere bekannte Knoten mit Schreibberechtigung *(Writers)* sowie eine vertrauenswürdige dritte Partei (*Trusted Third Party,* kurz TTP) gibt, welche als Transaktionsvermittler fungieren könnte. Jede dieser grundlegenden Fragen könnte zu einer schnellen Entscheidung gegen Blockchain führen. Die Unterscheidung zwischen permissionless und permissioned Blockchain erfolgt anhand der Fragen, ob alle schreibberechtigten Knoten im Netzwerk bekannt und für alle Netzwerkteilnehmer vertrauenswürdig sind. Sind alle schreibberechtigten Knoten bekannt, jedoch nicht alle vertrauenswürdig, wird zusätzlich zwischen *public permissioned Blockchains* und *private permissioned Blockchains* unterteilt. Unterschieden wird dabei, ob alle Knoten im Netzwerk einen Lesezugriff erhalten, um alle Zustände der Blockchain zu verifizieren oder nur definierte Knoten mit Leseberechtigung vorhanden sind, welche jeweils für sie bestimmte Transaktionen verifizieren können [3].

Die dargestellten Entscheidungskriterien geben einen klaren Hinweis darauf, ob die Blockchain-Technologie im Allgemeinen für den vorgesehenen

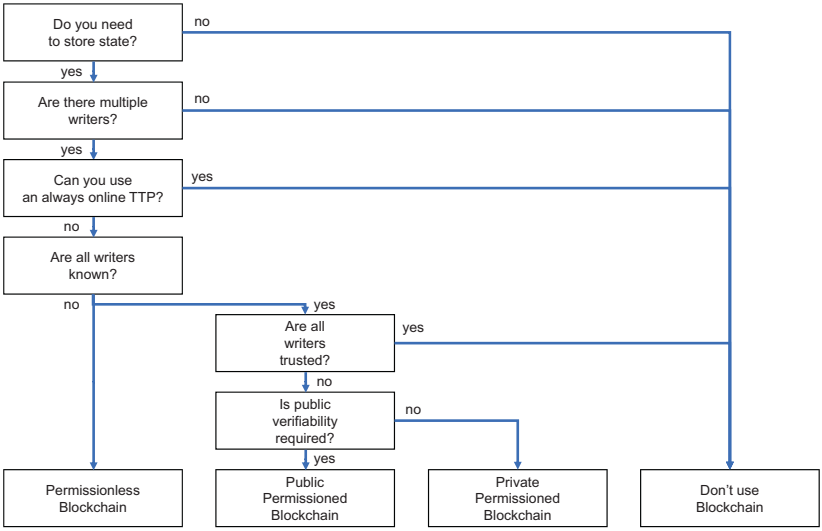

Abb. 3.2 Entscheidungsbaum nach Gervais und Wüst. (Eigene Darstellung in Anlehnung an Gervais/Wüst 2017, S. 3)

Anwendungsfall verwendbar ist. Das Modell bietet die Möglichkeit, nicht durchführbare Anwendungsfälle frühzeitig im Entscheidungsprozess von Organisationen zu stoppen. Obwohl die Bewertung anhand der dargestellten, abstrakten Sicht auf einem hohen Level erfolgt, reicht sie dennoch zur Bestätigung aus, ob dieser Anwendungsfall weiter tiefgreifend analysiert werden sollte. Hier ist es nun notwendig, den Anwender in weiteren Schritten über detailliertere Ebenen durch die verschiedenen, technologisch möglichen Blockchain-Konfigurationen zu führen, um die Kernanforderungen an den Anwendungsfall abzuprüfen.

Bedarf für ein neues Modell Aufgrund der bisherigen Argumentation ist die Blockchain-Technologie als radikale Innovation, oft verbunden mit einer strategischen Rolle, anzusehen. Die Architektur ist weitreichender als herkömmliche IT-Implementierungen (siehe Abschn. 2.3) und bedarf demnach eines Blockchain-spezifischen Modells. Dies wird teilweise in den Arbeiten von Graham sowie Gervais und Wüst dargestellt. Auch wenn letzteres Modell zu einem detaillierteren Ergebnis, als das von Graham, führt, ist für beide Versionen die Einbindung eines Blockchain-Experten notwendig. Insbesondere, da viele

technologische sowie organisatorische Aspekte in den Modellen nicht aufgegriffen werden, sollte für die Evaluierung aktive Expertenunterstützung hinzugezogen werden.

Tab. 3.1 gibt hierzu nochmals einen Überblick der berücksichtigten Kriterien je Modell und dient als Orientierung für das umfassende Modell in Abschn. 3.3 Es ist klar ersichtlich, welche Kriterien berücksichtigt wurden und an welchen Stellen eine weitere Vertiefung des Modells notwendig ist. Weiterhin wird die Hybrid-Blockchain in den analysierten Modellen nicht als mögliche Lösung angeboten, wenngleich diese Variante, als Kombination aus offenem und privatem Netzwerk, besonders für geschäftliche Ökosysteme zunehmend ein verstärktes Interesse erweckt und einen großen Mehrwert erbringen kann [4, 5].

Zusammengefasst ergibt sich der Bedarf, ein neues, ganzheitliches Modell für die Evaluierung zu entwickeln. Basierend auf den in der Literatur gewonnenen Erkenntnissen wird ein solches Modell in im folgenden Kapitel nachvollziehbar konstruiert.

Tab. 3.1 Übersicht der untersuchten Kriterien in den Modellen, (vgl. Hamilton et al. 2018), (vgl. Graham 2018), (vgl. Gervais/Wüst 2017)

Kriterium	IBM (Fragen)	Graham	Gervais und Wüst
Datenspeicherung?	Ja	Ja	Ja
Manipulationssicherheit und Transparenz/ Nachvollziehbarkeit?	Nein	Nein	Nein
Mehrere schreibende Parteien?	Ja	Ja	Ja
Sind diese bekannt?	Nein	Nein	Ja
Wird diesen vertraut?	Ja	Ja	Ja
Kann eine TTP genutzt werden?	Ja	Ja	Ja
Verifikation durch jeden?	Nein	Nein	Ja
Transaktion = Interaktion zwischen Teilnehmern?	Ja	Ja	Nein
Unterscheidung permissionless und permissioned Blockchain?	Nein	Nein	Ja
Unterscheidung private und public Blockchain	Nein	Nein	Ja
Einbindung Hybrid Blockchain?	Nein	Nein	Nein

3.3 Lösung – Das Blockchain-Entscheidungsmodell

Ziel des Entscheidungsmodells ist es, Manager, Innovatoren und Entscheider aus den Fachbereichen dabei zu unterstützen, potenzielle Blockchain-Anwendungsfälle im Vorfeld fundiert zu bewerten, um auf dieser Grundlage erste Ideen priorisieren zu können. Um dem gerecht zu werden, soll das Entscheidungsmodell zu einem interpretierbaren Ergebnis führen. Es soll auch für nicht Blockchain-Experten verständlich und ansprechend sein sowie ein ganzheitliches Bild der Anwendungsidee abdecken können. Aufgrund dieser Anforderungen wird das Entscheidungsmodell als Flussdiagramm entwickelt, in dem die einzelnen Kriterien anhand von Ja-Nein-Fragen geprüft werden. Die Kriterien selbst sollten möglichst allgemein verständlich (IT-Fachbegriffe sind weitestgehend zu vermeiden) und nach fachlichem Kontext sinnvoll gruppiert sein. Mithilfe dieses Modells wird ein möglicher Anwendungsfall auf seine Blockchain-Machbarkeit anhand organisatorischer sowie technologischer Kriterien bewertet. Als Resultat gibt das Modell neben dem Ergebnis, ob eine Idee grundsätzlich relevant für Blockchain ist, auch Auskunft darüber, welche Art der Blockchain ggf. optimal einsetzbar ist. Dieses Ergebnis kann als Fundament für eine Konzeption in Zusammenarbeit mit einem fundierten Blockchain-Experten dienen.

Modellentwicklung und Aufbau Folgend wird das Modell selbst aufgebaut, indem zunächst die relevanten Kriterien aus Abschn. 3.2 abgeleitet werden und diese in verschiedenen Gruppen den Gesamtrahmen des Modells ergeben. Dabei wird zusätzlich zwischen Soll- und Kann-Kriterien unterschieden. Als *Soll-Kriterien* werden solche bezeichnet, die erfüllt sein sollten, um Blockchain überhaupt als sinnvolle Technologie einsetzen zu können. Das Erfüllen von *Kann-Kriterien* hebt hingegen besonders geeignete Anwendungsfälle hervor, schließt bei Nichterfüllung jedoch keine Idee vollständig aus.

Auf Basis der vorhandenen Kriterien (vgl. Abschn. 3.2) können grundsätzlich die folgenden drei Kriterien-Gruppen *Organisationsstruktur, Technologie* sowie *Transaktionsdaten und Rechtesystem* unterschieden werden. Ziel der ersten beiden Gruppen ist es, grundlegend zu prüfen, ob Blockchain als geeignete Technologie zum Einsatz kommen sollte. Die dritte Gruppe legt ergänzend den Fokus auf die Prüfung von Konfigurationsideen in Bezug auf die Datenverarbeitung und das Rollen- und Rechtesystem und identifiziert nicht realisierbare Kombinationen von Anforderungen. Letztendlich soll sich der Anwender

über mögliche organisatorische Risiken und Veränderungen bewusstwerden (erste Gruppe), bevor er Transparenz über erste technische Möglichkeiten der Blockchain-Architektur erhält (entspricht der zweiten Gruppe). Die dritte Gruppe gibt zusätzlich Einsicht in mögliche Blockchain-Konfigurationen bzgl. der Datenverarbeitung und den Zugriffsrechten.

Gruppe 1: Organisationsstruktur Die erste Gruppe beschreibt die Organisationsstruktur. Das heißt, wer sind die potenziellen Teilnehmer, welche Art der Zusammenarbeit herrscht im Ökosystem vor und wie sieht deren Transaktions- und Vertrauensverhältnis aus. Dabei soll eine ganzheitliche Sicht auf die geschäftlichen Beziehungen im Sinne des Austauschs von Transaktionen gewonnen werden.

Grundvoraussetzung, damit eine Blockchain-Lösung organisatorisch sinnvoll und der Aufbau finanzierbar ist, stellt das Vorhandensein einer ausreichenden Anzahl an Netzwerkteilnehmern dar [6]. Zur genauen Anzahl, ab wann Blockchain für die Teilnehmer einen wirklichen Mehrwert bringt, gibt es in der Literatur unterschiedliche Angaben. Generell lässt sich jedoch festhalten, dass der Mehrwert für das Geschäftsnetzwerk mit steigender Teilnehmeranzahl in der Regel ebenfalls steigt, denn je mehr Teilnehmer des gegenwärtigen Geschäftsökosystems Teil des Blockchain-Netzwerkes sind, desto weniger Transaktionsverbindungen werden außerhalb der Blockchain benötigt. Das DLT-Netzwerk wird somit für die einzelne Organisation zur *Single Source of Truth* und zum *Single Point of Access,* ohne jedoch eine zentralisierte Lösung zu etablieren. Grundsätzlich ist jedoch festzuhalten, dass mindestens drei Netzwerk-Teilnehmer sinnvoll sind, da bei nur ein bis zwei Teilnehmern eine zentrale oder geteilte Datenbank zumeist organisatorisch besser händelbar ist. Blockchain-Anwendungen können zum Teil auch bereits bei einer geringen Teilnehmeranzahl sinnvoll sein, wenn diese einen gemeinsamen und vertrauenswürdigen Konsens benötigen.

Aufgrund der Architektur (vgl. Abschn. 2.2) schafft Blockchain vertrauensvolle und nachvollziehbare Transaktionen zwischen Organisationen, die sich bisher nicht vertrauen. Dieses in der realen Welt vielmals fehlende Vertrauensverhältnis kann demnach mit als Soll-Kriterium für einen Blockchain-Anwendungsfall betrachtet werden.

Daraus ergibt sich im nächsten Schritt die Frage nach dem Wegfall von Intermediären als zentrale Vertrauensstelle innerhalb der Transaktion. Aufgaben, die bisher bspw. von Banken übernommen wurden, lassen sich nun auf Basis der Architektur lösen. Zudem verringern sich damit oftmals parallel die Transaktionskosten und Durchlaufzeiten [7]. In Summe ist die Blockchain-Technologie sinnvoll, wenn es keine zentrale Vertrauensstelle gibt bzw. die existierende ZVS

abgeschafft werden soll oder grundsätzlich Konflikte darüber auftreten, welche Organisation als ZVS agiert. Einen weiteren Vorteil bringt ein Anwendungsfall mit sich, wenn die bisherige ZVS zusätzlich zu Ineffizienzen oder verlängerten Prozessdurchlaufzeiten geführt hat (Kann-Kriterium).

Bei allen Vorteilen der Dezentralisierung, erschwert sie aber zugleich die Verteilung bzw. Umsetzung neuer Geschäftsregeln innerhalb des Netzwerkes (Verteilung neuer Smart Contracts). Ändern sich diese häufig, ist damit zwar ein erhöhter Aufwand verbunden, schließt Blockchain als Lösung jedoch nicht aus. Daher wird dies im Modell als weiteres Kann-Kriterium aufgenommen.

Gruppe 2: Technologie Das zweite Cluster prüft die technologischen Anforderungen an den Anwendungsfall und ob sich diese grundsätzlich mit einer Blockchain realisieren lassen. Aufgrund der Mechanismen zur Konsensfindung durch die Smart Contracts (vgl. Abschn. 2.2) ist die Validierung und Durchführung einer Transaktion mit einem gewissen Aufwand verbunden. Für Massentransaktionen wie bspw. Kreditkartenzahlungen ist Blockchain nach dem heutigen Stand nicht geeignet, da die Skalierung dafür gegenwärtig noch nicht ausgelegt ist [8].

Kerneigenschaft und Kriterium ist weiterhin der gemeinsame Konsens zwischen allen Netzwerkteilnehmern, der auf Basis der Architektur durch den Shared Ledger erzeugt wird. Auf dieser Grundlage ist es zumeist jedem Teilnehmer möglich, die Inhalte der Blockchain zu verifizieren und die Originalität der Daten nachzuprüfen. Hierbei ist zu beachten, dass je nach Blockchain-Framework nicht zwangsläufig jeder Teilnehmer berechtigt ist, auch alle Transaktionsinhalte zu lesen. Die Verifikation der Daten kann jedoch auch ohne Leseberechtigung der Daten erfolgen, indem bspw. der Hashwert selbst sowie die Signatur verifiziert werden [3]. Einzelne Transaktionen und Werte können im Nachhinein nur durch eine Gegenbuchung, die ebenfalls als Transaktion in einem Block festgehalten ist, verändert werden. Geschriebene Daten können entsprechend nicht direkt manipuliert werden [6]. Diese beiden Kriterien (gemeinsamer Konsens und nicht Manipulierbarkeit der Daten) sind zwar Kerneigenschaft der Blockchain, jedoch sind nicht beide unbedingt zwingend gleichzeitig zu erfüllen, damit ein Anwendungsfall sinnvoll ist. Vielmehr genügt es bereits, dass eines von beiden zutrifft. Ein Beispiel stellt der Austausch von Statusinformationen dar. Es ist zwar wichtig, dass alle Teilnehmer die gleiche Sicht auf den aktuellen Status haben, den gemeinsamen Konsens bilden, nicht jedoch ist es zwingend erforderlich, den Status der Vergangenheit manipulationssicher vorzuhalten.

Auf Grundlage der technischen Funktionsweise wird der Bedarf für Datensicherungen durch Redundanz als Kann-Kriterium ergänzt. Bisher werden Backups meist als Kopie des bestehenden Datenbestandes auf andere Datenträger gezielt durchgeführt.[1] Der Shared Ledger einer Blockchain liegt hingegen verteilt als vollständige Kopie bei jedem Knotenbetreiber (aktiver Teilnehmer) des Netzwerkes. Somit sind theoretisch keine zusätzlichen Maßnahmen zur Datensicherung erforderlich, da die Nutzdaten selbst aufgrund der Architektur automatisch gesichert werden [9].

Wie oben bereits erwähnt, kann das Blockchain-Netzwerk als *Single Point of Access* agieren, wenn neben diesem Netzwerk keine weiteren Schnittstellen zum Datenaustausch innerhalb des Ökosystems erforderlich sind. Wird bspw. eine Lieferkette mit allen Akteuren als Blockchain-Netzwerkes abgebildet, wird die heutige Komplexität reduziert, indem der Betrieb mehrerer, paralleler Schnittstellen entfällt. Weiterhin wird Informationsasymmetrien vorgebeugt, da alle Akteure zur gleichen Zeit den gleichen Informationsstand besitzen (Kann-Kriterium).

Auf die Empfehlung eine (de-) zentrale Datenbank zu nutzen, wird in dem Modell bewusst verzichtet, da hierfür jeweils weitere Kriterien zur Unterscheidung erforderlich sind und zu einem explizierten Entscheidungsbaum für zentrale oder dezentrale Datenbanken führen. Um die Anwendbarkeit des Modells sicherzustellen, wird der Fokus des Entscheidungsmodells darauf gelegt zu prüfen, ob sich Blockchain für den Anwendungsfall generell als Technologie eignet.

Gruppe 3: Transaktionsdaten und Rechtesystem Nachdem der Anwendungsfall in den beiden ersten Clustern bereits auf die grundsätzliche Blockchain-Relevanz geprüft wurde, wird in Cluster drei eine konkrete Unterscheidung der einzelnen Konfigurationen der Blockchain vorgenommen, die als konkretes Ergebnis für den Anwender dienen. Insbesondere werden die Anforderungen an das Rollen- und Rechtesystem auf Grundlage der Datenzugriffe bzw. Freigaben herausgestellt.

Zur Unterscheidung der verschiedenen möglichen Arten der Blockchain wird auf den Entscheidungsbaum von Gervais und Wüst zurückgegriffen, da hier bereits permissioned und permissionless sowie private und public Blockchain eingeführt

[1] RAID (Redundant Array of Independent Disks) beschreibt ein Verfahren zur redundanten Datenspeicherung auf mehreren physischen Festplatten. Ziel ist es, die Performance, Fehlertoleranz sowie Datensicherheit zu erhöhen. Das Verfahren findet bis heute Anwendung [12].

und unterschieden werden [3]. Ergänzt wird diese Unterteilung noch um Hybrid-Blockchains, die eine Kombination aus einer permissioned und permissionless Blockchain darstellen, indem mehrere Blockchains parallel betrieben und miteinander verknüpft werden. Der Vorteil besteht darin, dass Daten einerseits offen mit jedem geteilt werden können, parallel jedoch für einzelne Geschäftstransaktionen in dem privaten, permissioned Teil verarbeitet werden [10]. Primär für Enterprise Lösungen rückt die Hybrid Blockchain immer stärker in den Fokus [4, 5]. Auch sollen Orakel als Schnittstelle zwischen der Blockchain und externen Datenquellen oder Systemen in die Lösungsvorschläge integriert werden. Mittels eines Orakel lässt sich bspw. auch auf externe Events, Echtzeitdaten oder andere Prozesse zugreifen und reagieren [11].

Zum besseren Verständnis der Unterscheidungsmerkmale der einzelnen Ausprägungen, fasst Tab. 3.2 die zu Beginn dieses Kapitels bereits angeführten Aspekte auf und stellt dar, in welchem Kriterium der wesentliche Unterschied liegt.

Das Blockchain-Entscheidungsmodell Zur zielgerichteten Untersuchung eines konkreten Anwendungsfalls, ist das Blockchain-Entscheidungsmodell (Abb. 3.3) als einseitiges Flussdiagramm dargestellt. Zuerst sind die Kriteriengruppen eins *(Organisationsstruktur)* und zwei *(Technologie)* zu durchlaufen. Beginnend bei *Start* sind die einzelne Fragen in Bezug auf den konkreten Anwendungsfall zu beantworten, wobei Blockchain hierbei als geeignete Technologie für das Anwendungsszenario bereits ausgeschlossen werden kann. Die vier

Tab. 3.2 Einteilung der Konfigurationsmöglichkeiten der Blockchain

Konfiguration	Unterscheidungskriterium
Hybrid Blockchain	Anwendungsfall erfordert einen öffentlichen (frei zugänglichen) und einen privaten Anteil
Permissioned – permissionless Blockchain	Sind alle schreibenden Teilnehmer bekannt, können diese klar identifiziert werden (permissioned) Sind Teilnehmer nicht bekannt oder es soll sich jeder frei mit der Blockchain verbinden können (permissionless)
Private – public Blockchain	Permissioned Blockchain: Kann jeder Teilnehmer alles sehen oder jeder nur für ihn speziell freigegebene Daten?
Orakel	Soll eine Schnittstelle zu externen Systemen oder Datenquellen vorhanden sein?

Kann-Kriterien (bzw. Bonus-Kriterien) der ersten beiden Gruppen kennzeichnen besonders sinnvolle Einsatzbereiche, schließen jedoch keine Anwendung aus. Sind die ersten beiden Gruppen vollständig durchlaufen, ohne das die Antwort auf eine der Fragen *Keine Blockchain* war, wird ausgehend von dem *UND-Feld* die Gruppe drei begonnen. Diese Gruppe schließt Blockchain als Technologie-Basis nicht mehr aus, sondern gibt eine Empfehlung ab, welche Art der Blockchain für das konkrete Einsatzszenario am geeignetsten ist. Das Vorgehen zur Beantwortung der einzelnen Fragen verhält sich analog zu den ersten beiden Gruppen.

Einzig mit dem Blockchain-Entscheidungsmodell nicht abgedeckter Anwendungsfall ist Blockchain als digitale Sicherung von geistigem Eigentum, Patenten oder sonstigen Dateien. Zum Nachweis, dass eine bestimmte Datei, z. B. Dokumentation über ein neues Forschungsergebnis, zu einem definierten Zeitpunkt im eigenen Besitz war, kann der Hashwert dieser berechnet und in einer permissionless Blockchain geteilt werden. Parallel ist die Datei im eigenen Zugriff unverändert zu speichern. Später kann jederzeit erneut der Hashwert dieser Datei gebildet werden und mit dem in der Blockchain hinterlegten Wert abgeglichen werden. Stimmen beide Werte überein, ist der Beweis erbracht, dass die Datei seit dem Eintrag im Shared Ledger nicht mehr verändert wurde. Insbesondere für Forschungsarbeiten, Paper oder Erfindungen vor Patentanmeldung stellt dieses Verfahren eine einfache und sehr sichere Methode dar, das eigene geistige Eigentum zu sichern. Selbst wenn ein Dritter die gleiche Forschungsarbeit durchführt, wird dieser keine bis auf das letzte Zeichen identische Dokumentation (inkl. der Meta-Daten der Datei) besitzen. Daher lässt sich der in der Blockchain hinterlegte Hashwert nur mit der ursprünglichen Originaldatei erzeugen. Die rechtliche Anerkennung dieser Methode ist gegenwärtig noch ungeklärt. Da dieser Anwendungsfall weder eine ZVS einbindet, noch ein Geschäftsnetzwerk zum Austausch von Transaktionen aufbaut ist das nachfolgend vorgestellte Entscheidungsmodell einzig hierfür nicht anwendbar.

Zum besseren Verständnis der Unterscheidungskriterien sowie zur Einordnung des eigenen Anwendungsszenarios, erläutert Tab. 3.3 die einzelnen Fragestellungen in einer zusammenfassenden Übersicht.

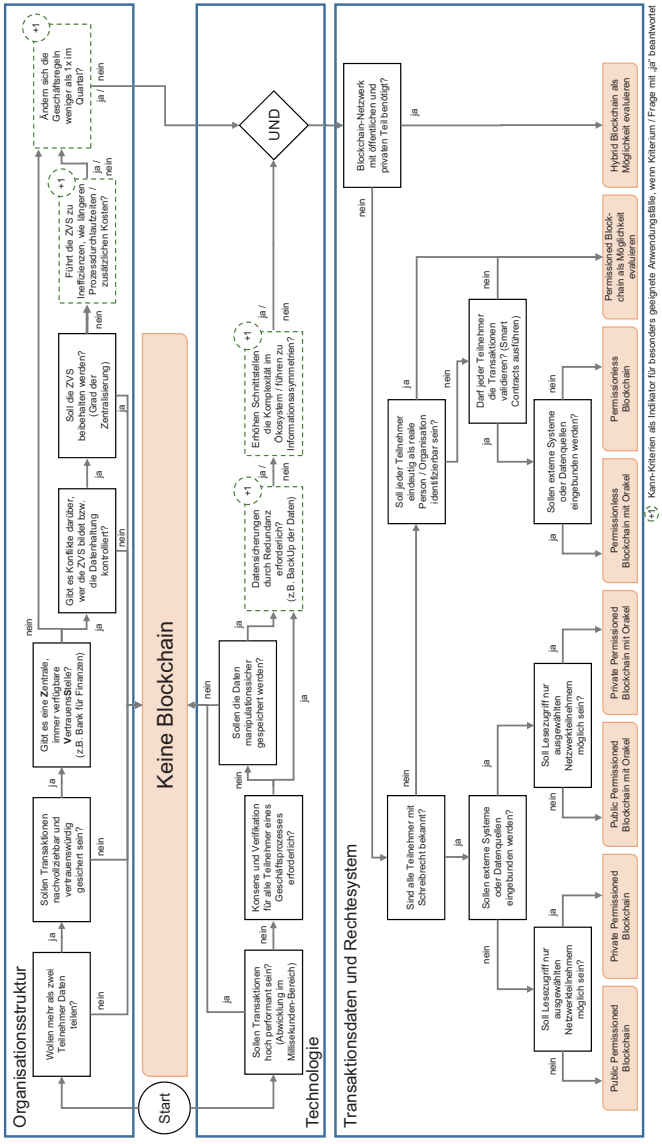

Abb. 3.3 Blockchain-Entscheidungsmodell. (Eigene Darstellung)

Tab. 3.3 Erläuterung der Entscheidungskriterien des Blockchain-Entscheidungsmodells

Gruppe	Unterscheidungskriterium	Erläuterung
Organisations-struktur	Wollen mehr als zwei Teilnehmer Daten teilen?	Da Blockchain als Netzwerk funktioniert und die Manipulationssicherheit sowie das damit verbundene Vertrauen erst durch mehrere lokale Kopien des Ledgers (der Blockkette) erreicht wird, sind min. drei Teilnehmer erforderlich.
	Sollen Transaktionen nachvollziehbar und vertrauenswürdig gesichert sein?	Die nachvollziehbare und vertrauenswürdige Datenspeicherung ist das Kernelement der Blockchain und gleichzeitig der Hauptvorteil dieser Technologie gegenüber anderen technologischen Lösungen, die dies zumeist nur sehr schwer bis gar nicht abbilden können.
	Gibt es eine **Z**entrale, immer verfügbare **V**ertrauens**S**telle? (z. B. Bank für Finanzen)	Eine zentrale Organisation die Transaktionen bzw. Geschäftsprozesse in einem Ökosystem bündelt, durch ihre Rolle als Vertrauensstelle fungiert und durch die anderen Organisationen anzuerkennen ist.
	Gibt es Konflikte darüber, wer die ZVS bildet bzw. die Datenhaltung kontrolliert?	Insbesondere mit zunehmender Komplexität des Geschäftsnetzwerkes (höhere Anzahl Teilnehmer) wird es schwerer, eine Organisation zu bestimmen, der alle Teilnehmer das Vertrauen zusprechen, sodass diese als ZVS agieren kann.
	Soll die ZVS beibehalten werden? (Grad der Zentralisierung)	s. o.
	Führt die ZVS zu Ineffizienzen, wie längeren Prozessdurchlaufzeiten/ zusätzlichen Kosten?	Gibt es eine ZVS, ist diese i. d. R. durch die weiteren Netzwerkteilnehmer zu finanzieren (z. B. durch Transaktionsgebühren) und führt zu einem Engpass in der Verarbeitungsgeschwindigkeit *(Flaschenhalsprinzip),* was sich insb. negativ auf die Skalierung von Prozessen auswirkt.
	Ändern sich die Geschäftsregeln weniger als 1x im Quartal?	Smart Contracts im Blockchain-Netzwerk validieren und prüfen jede einzelne Transaktion vor ihrer Durchführung. Voraussetzung hierfür ist, dass sich alle Netzwerkteilnehmer auf eine Version des Smart Contracts einigen, die bei jeder Aktualisierung durch diese zu akzeptieren ist. Die vermehrte Anpassung der Geschäftslogik führt somit zu einem höheren Aufwand in der Aktualisierung der Smart Contracts im Netzwerk.

(Fortsetzung)

Tab. 3.3 (Fortsetzung)

Gruppe	Unterscheidungskriterium	Erläuterung
Technologie	Sollen Transaktionen hoch performant sein? (Abwicklung im Millisekunden-Bereich)	Vorgänge wie z. B. Kreditkartenzahlungen oder das Speichern von Sensordaten in der Cloud sind Vorgänge, die viele Transaktionen in einem sehr kurzen Zeitraum erfordern. Aufgrund der typischen Blockchain-Architektur (verteilen und validieren der Transaktionsanfragen im Netzwerk sowie Berechnung und Verteilung der neuen Blöcke) benötigt die Verarbeitung eine gewisse Zeit, wodurch sie gegenwärtig nicht für hochperformante Massentransaktionen geeignet ist.
	Konsens und Verifikation für alle Teilnehmer eines Geschäftsprozesses erforderlich?	Ein Kernelement der Blockchain-Technologie ist es, einen gemeinsamen Konsens (Datenstand) über das gesamte Netzwerk hinweg zu schaffen sowie es den Teilnehmern zu ermöglichen, Datenstände und Transaktionen im Nachhinein zu validieren.
	Sollen die Daten manipulationssicher gespeichert werden?	Ebenfalls Kernelement der Blockchain-Technologie ist die manipulationssichere Datenspeicherung. Ist eine Transaktion einmal im Netzwerk geschrieben, kann sie nur noch durch eine Gegenbuchung, nicht jedoch durch eine Änderung der Transaktion an sich, geändert werden. Basis dafür ist der Hashwert jedes Blocks, die Verkettung der Blöcke untereinander anhand der Hashwerte sowie die verteilte Speicherung der Blockkette auf den Netzwerkknoten.
	Datensicherungen durch Redundanz erforderlich? (z. B. BackUp der Daten)	Da jeder aktive Netzwerkteilnehmer eine eigene lokale Kopie der Blockkette (Transaktionshistorie) vorhält, könnte auf die traditionelle Datensicherung durch Redundanz verzichtet werden. Fällt der eigene Netzwerkknoten aus, kann ein neuer aufgesetzt und in das Netzwerk eingebunden werden. Sobald sich dieser im Netzwerk befindet, kann die aktuelle, vollständige Blockkette lokal repliziert werden und der Ausgangszustand (plus die Transaktionen, die in der Zwischenzeit erfolgt sind) wieder hergestellt werden.
	Erhöhen Schnittstellen die Komplexität im Ökosystem/ führen zu Informationsasymmetrien?	Für den gegenwärtigen Datenaustausch betreiben Organisationen zumeist eine Vielzahl verschiedener Schnittstellen zu unterschiedlichen externen Partnern, die einerseits die Komplexität erhöhen, jedoch zugleich zu Informationsasymmetrien führen, da unterschiedliche Partner Datenaktualisierungen ggf. zu unterschiedlichen Zeitpunkten erhalten.

(Fortsetzung)

Tab. 3.3 (Fortsetzung)

Gruppe	Unterscheidungskriterium	Erläuterung
Transaktionsdaten und Rechtesystem	Blockchain-Netzwerk mit öffentlichen und privaten Teil benötigt?	Wird ein öffentlicher und privater Netzwerkteil innerhalb eines Anwendungsfalls benötigt, können beide Blockchain-Netzwerke als Hybrid-Blockchain zusammengeführt werden.
	Sind alle Teilnehmer mit Schreibrecht bekannt?	Sind alle Netzwerkteilnehmer mit Schreibrecht bekannt, so kann ein privates (permissioned) Blockchain-Netzwerk genutzt werden. Wird mit unbekannten Dritten gearbeitet, ist zwangsläufig auf öffentliche (permissionless) Blockchain-Netzwerke zurückzugreifen.
	Soll jeder Teilnehmer eindeutig als reale Person/Organisation identifizierbar sein?	Die eindeutige Zuordnung eines technischen Netzwerkknoten zu einer realen Person kann nur in permissioned Blockchain-Netzwerken sichergestellt werden. In öffentlichen Netzwerken können KYC[a] Prozesse eingesetzt werden, die aber gegenwärtig eher eine Ausnahme darstellen und nativ nicht in der Blockchain-Architektur vorgesehen sind.
	Darf jeder Teilnehmer die Transaktionen validieren? (Smart Contracts ausführen)	Typischerweise verfügt jeder Netzwerk-Teilnehmer innerhalb der öffentlichen Blockchain über identische Rechte. In permissioned Implementierungen können hingegen spezifische Rechte je nach Teilnehmer vergeben werden, die auch die Ausführung der Smart Contracts umfassen können.
	Sollen externe Systeme oder Datenquellen eingebunden werden?	Orakel bilden die Schnittstelle zwischen dem Blockchain-Netzwerk und anderen, Dritten Systemen. Über Orakel können Daten aus der Blockchain nach Außen weitergegeben werden oder eben von Netzwerk-externen Datenquellen abgerufen werden.
	Soll Lesezugriff nur ausgewählten Netzwerkteilnehmern möglich sein?	In der zugriffsbeschränkten (permissioned) Blockchain kann jeder Teilnehmer mit spezifischen Rechten versehen werden, die auch die Leserechte auf bestimmte Transaktionsdaten umfassen.

[a]KYC steht für *Know Your Customer* (zu Deutsch, wörtlich: *Kenne Deinen Kunden*) und bezeichnet eine oft vom Gesetzgeber vorgeschriebene Legitimationsprüfung für (Neu-) Kunden, insbesondere für Banken und Versicherungen. Ziel ist die Verhinderung von Geldwäsche, indem die Identität des Kunden eindeutig verifiziert und sichergestellt wird.

3.4 Fazit – Blockchain-Entscheidungsmodell

Wie in den vorherigen Abschnitten dargelegt, ergeben sich erfolgreiche Anwendungsfälle aus dem Zusammenwirken verschiedener organisatorischer, als auch technischer Kriterien. Das Entscheidungsmodell gibt Anwendern die Möglichkeit, den persönlichen Anwendungsfall in einem strukturierten und transparenten Rahmen auf die Relevanz für den Einsatz der Blockchain-Technologie zu prüfen. Zudem führt das Modell eine Argumentation an, warum Blockchain sich für den spezifischen Anwendungsfall im Besonderen eignet und herkömmlichen Technologie-Ansätzen überlegen ist.

Die Verwendung des Entscheidungsmodells setzt voraus, dass der Nutzer sowohl mit dem organisatorischen, als auch mit dem technischen Hintergrund des Anwendungsfalls vertraut ist und diesen entsprechend beurteilen kann. Primär dient das Modell zur Prüfung eines potenziellen Anwendungsfalls auf die Relevanz für den Einsatz von Blockchain, jedoch nicht, um aus den vorliegenden Kriterien einen potenziellen Anwendungsfall oder ein potenzielles Einsatzgebiet zu konstruieren. Auch wird vorausgesetzt, dass der Nutzer über erstes Basiswissen zum Thema Blockchain verfügt, damit das inhaltliche Verständnis für die Kriterien sichergestellt ist.

Literatur

1. Hamilton, M./Harrison, K./Lowry, E./Widdifield, J. (2018). *The Founder's Handbook – Your guide to getting started with blockchain.* Armonk: IBM Corporation.
2. Graham, W. (05. Februar 2018). *Building it Better: A Simple Guide to Blockchain Use Cases*. Abgerufen am 26. April 2018 von Blockchain at Berkeley: https://blockchainatberkeley.blog/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60
3. Gervais, A./Wüst, K. (2017). *Do you need a Blockchain?* Zurich: ETH Zurich.
4. Canterbury, J./Morrell, B. (2017). *Product life cycle management on a blockchain network*. o. O.: EY.
5. Khekade, A. (20. Januar 2018). *If you Thought Blockchain was Amazing, Wait till You Read about Hybrid Blockchain*. Abgerufen am 26. Mai 2018 von Entrepreneur India: https://www.entrepreneur.com/article/307794
6. Burghardt, T./Krause, E./Nack, D./Schmidt, M./Treder, T.-M./Velamuri, V. (2016). *Blockchain Technology and the Financial Services Market - State-of-the-Art Analysis*. Leipzig: Infosys Consulting.
7. Prinz, W. (2017). *Blockchain Potentiale und Anwendungen.* Sankt Augustin: Fraunhofer FIT.

8. Gantner, T./Nack, D./Schwarz, M./Schwarz, R./Winkler, J. (2017). *Blockchain: Die Demokratisierung des Gesundheitswesens?* Leipzig: Wissenschaftliches Institut für Gesundheitsökonomie und Gesundheitssystemforschung.
9. Evans-Greenwood, P./Harper, I./Hillard, R./Williams, P. (2016). *Bitcoin, Blockchain, and Distributed Ledgers: Caught between promise and reality.* o. O.: Deloitte.
10. The Institutes. (2017). *Blockchain Building Blocks: Creating a world of opportunity for insurance from an evolving area of technology*. Malvern: The Institutes.
11. Kakavand, H./Kost De Sevres, N. (2016). *The Blockchain Revolution: An Analysis of Regulation and Technology related to distributed Ledger Technologies*. o. O.: o. V.
12. Rouse, M. (2016). *RAID (Redundant Array of Independent Disks).* Abgerufen am 10.10.2019 von Searchstorage: https://www.searchstorage.de/definition/RAID-Redundant-Array-of-Independent-Disks

Mehrwerte für Netzwerkteilnehmer

4

Im vorherigen Kapitel wurden potenzielle Blockchain-Anwendungsfälle auf Grundlage des Blockchain-Entscheidungsmodells auf ihre Relevanz für den Einsatz dieser Technologie geprüft. Weiterhin lässt sich mit dem vorgestellten Modell die am besten geeignete Blockchain-Variante identifizieren. Stellt sich eine Anwendungsidee als sinnvoll und geeignet dar, gilt es nun, den Mehrwert klar zu identifizieren. Zum einen ist die Wirtschaftlichkeit vor der Umsetzung eines neuen Projektes in vielen Unternehmen klar aufzuzeigen. Zum anderen lassen sich potenzielle Teilnehmer bei einem konkret aufgezeigten Mehrwert einfacher überzeugen, sich dem Netzwerk, bzw. dem Projekt anzuschließen. Da Blockchain auf dem Netzwerkgedanken beruht, ist insbesondere der zweite Schritt, mehrere initiale Teilnehmer zu gewinnen, essenziell für die weitere Entwicklung sowie den weiteren Erfolg der Anwendungsidee.

Insbesondere die Frage nach dem Mehrwert der Blockchain sowohl für die einzelne Organisation, als auch für das gesamte Netzwerk spielt im Rahmen der Projektumsetzung oftmals eine entscheidende Rolle. Die Skalierung vieler als Proof-of-Concept gestarteter Pilotprojekte scheitert an der organisatorischen Skalierung. Oft erkennen weitere Organisationen innerhalb des etablierten Geschäftsnetzwerkes (ohne Blockchain als gemeinsame Kommunikationsbasis) den erzielbaren Mehrwert durch den Einsatz von Blockchain nicht bzw. nehmen aus anderen Gründen Abstand von einer Teilnahme an dem Netzwerk. Mit einer gezielten Definition des Mehrwertes lässt sich dem entgegenwirken. Zeitgleich ist eine Abgrenzung zum Hype, die neue Technologie einzusetzen, möglich, indem der wirtschaftliche Wert über den technologischen Reiz gestellt wird.

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_4

Zur Beantwortung der zweiten zentralen Fragestellung:

Inwiefern kann der Mehrwert von Blockchain für die Netzwerkteilnehmer qualitativ beschrieben werden?

Wird in diesem Kapitel zunächst der Mehrwertbegriff definiert sowie mögliche Variationen und Darstellungsformen betrachtet (Abschn. 4.1). Im nächsten Schritt wird, maßgeblich basierend auf Literaturangaben, der grundsätzliche Mehrwert, der sich aus der Natur der Blockchain ergibt, aufgezeigt (Abschn. 4.2). Da der Mehrwert immer im Zusammenhang mit dem konkreten Anwendungsfall steht, wird anschließend der qualitative Mehrwert anhand zweier Praxisbeispiele evaluiert (Abschn. 4.3). Abschließend wird darauf aufbauend ein Modell vorgestellt, mit dem sich die Aspekte des qualitativen Mehrwertes systematisch für eine spezifische Anwendungsidee bestimmen lassen (Abschn. 4.4).

4.1 Mehrwerttheorien

Grundsätzlich ist der Mehrwertbegriff allgemein bekannt, wird aber unterschiedlich interpretiert. Die Interpretation hängt davon ab, ob eher quantitative oder qualitative Sichten die Bewertung beeinflussen. Aufgrund dessen wird die Definition des Mehrwertes nachfolgend auf Grundlage verschiedener Mehrwerttheorien hergeleitet.

Exkurs: Ursprung der Mehrwerttheorien

Basierend auf der sozialistischen Wirtschaftslehre, geprägt durch Karl Marx, bezeichnet Mehrwert einen von dem Kapitalisten unentgeltlich angeeigneter Wert. Im kapitalistischen Produktionsprozess schafft der Lohnarbeiter diesen über den Wert der Arbeitskraft hinaus. Als Quelle des Mehrwertes wird die menschliche Arbeitskraft bezeichnet, die innerhalb eines Arbeitstages eine über den eigenen Bedarf hinausgehende Menge von Produkten erzeugen kann. Der Mehrwert spiegelt die Differenz zwischen der insgesamt geleisteten Arbeitskraft und der für die Reproduktion der eigenen Arbeitskraft (durch das Gehalt abgebildet) eingesetzte Arbeitskraft wider [1]. Um den Mehrwert zu erhöhen, leiten sich zwei Ansätze ab:

1. Die Arbeitszeit wird verlängert und damit die Zeit der Mehrwertproduktion verlängert (absoluter Mehrwert).
2. Durch Intensivierung der Arbeitstätigkeit (relativer Mehrwert) werden mehr Produkte im gleichen Zeitraum, mithilfe technischer Unterstützung, erzeugt.

Zwar soll in der Folge der Mehrwert nicht als reine Mehrleistung menschlicher Arbeit betrachtet werden, dennoch stützen sich heutige Mehrwerttheorien primär auf den relativen Mehrwert. Insbesondere der Grundgedanke des Deltas, indem mehr Output mit gleichem oder gar geringerem Input erzeugt werden kann, ist relevant.

Joseph Schumpeter, der gleichzeitig als Vater der Innovationstheorien gilt, beschreibt Schumpetersche Renten. Diese Renten gelten als die Gewinne, die zwischen der Einführung einer Innovation und ihrer erfolgreichen Verbreitung entstehen. Gemeint ist damit der Überschuss, der die anfallenden Kosten für die Produktion des erwünschten Outputs übersteigt. Schumpeter nimmt an, dass erfolgreiche Innovationen im Laufe der Zeit imitiert werden. Bis zu diesem Zeitpunkt bilden sich die Schumpeterschen Renten, auch als Unternehmerrente bezeichnet. Die Einnahmen erhöhen sich kurzfristig über ihre Ressourcenkosten hinaus [2]. Schumpeter beschreibt Innovationen als neue Kombination oder Rekombination von Faktoren, z. B. neuer Technologien. Diese führen zu neuen Gütern, neuen Märkten, neuen Produktionsmethoden oder neuen Bezugsquellen [3]. ◀

Parallel zu diesen Theorien hat Ronald Coase das Konzept der Transaktionskostenökonomie (Englisch: Transaction Costs Economics, kurz TCE) eingeführt. Coase argumentiert, dass Unternehmen aus ökonomischer Sicht nur dann sinnvoll sind, wenn sie die Transaktionskosten reduzieren oder eliminieren [4]. Die TCE kann als Theorie der organisatorischen Effizienz angesehen werden. Ziel ist die vergleichsweise bessere Organisation für eine konkrete Aufgabe zu identifizieren. Kernziel ist es, eine organisatorische Lösung für die spezifische Transaktion zu finden, um diese so effizient wie möglich, respektive zu den geringsten Kosten, abzubilden [5]. Es wird davon ausgegangen, dass der untersuchten Organisation Faktormärkte vorangehen und Absatzmärkte nachgelagert sind. Die Organisation bewegt sich folglich in einem Netzwerk. In Bezug auf die Organisation der Transaktionen wird die vertikale und horizontale Integration unterschieden. Ist die unternehmenseigene Koordination der Transaktionen kostengünstiger umsetzbar, als extern über den verfügbaren Markt, wird dies eine Verlagerung ökonomischer Aktivitäten in das eigene Unternehmen zur Folge haben (vertikale Integration). Im Gegenzug wird die Verlagerung von Transaktionen aus dem Unternehmen in den Markt erfolgen, wenn die internen Organisationskosten steigen und die Grenzkosten des Unternehmens die des Marktes übersteigen (horizontale Integration). Vorausgesetzt, es wird nicht aus strategischen Zwecken auf eine vertikale Integration gesetzt, um z. B. Konkurrenten den Zugang zu Wissen zu erschweren [6]. Abb. 4.1 illustriert diese Integrationsstufen schematisch.

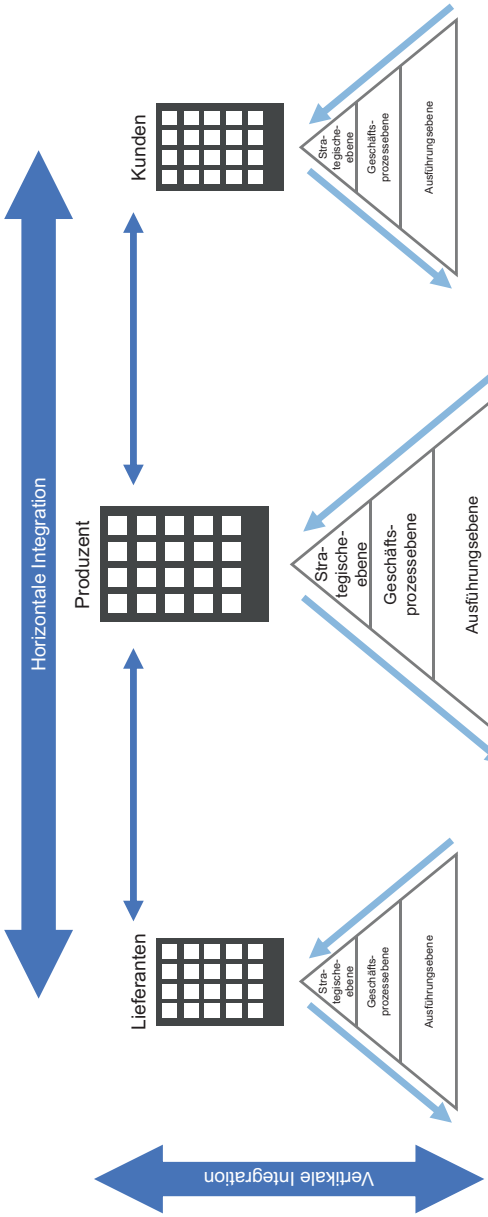

Abb. 4.1 Horizontale und vertikale Integration in Geschäftsnetzwerken. (Eigene Darstellung)

Faktisch ist Effizienz eine Hauptquelle der Transaktionskostenökonomie. Eine gesteigerte Effizienz verringert die Kosten und initiiert die Schumpeterschen Renten. Zusätzlich können die Reduktion von Komplexität und Informationsasymmetrie sowie die Existenz von Vertrauen die Effizienz steigern. In Verbindung mit einer Senkung der Transaktionskosten, ergibt sich hieraus die Wertschöpfung [7].

Das Aufkommen der Informationstechnologie und einer gesteigerten Internetnutzung haben die Transaktionskosten maßgeblich beeinflusst. Das Aufheben von Beschränkungen, bspw. einer Informationsasymmetrie oder einer eingeschränkten Austauschfrequenz, führt zu einer verbesserten Effizienz. Direkte Auswirkungen auf die Kosten ergeben sich, indem bspw. Portokosten entfallen [8].

> „Die Einflussnahme von IT auf die Leistung eines Unternehmens ist unbestritten. Dennoch bleibt die Frage nach den wesentlichen Stellhebeln, die eine vorteilhafte Nutzung ermöglichen." [9]

Oft stehen im Zusammenhang mit der Nutzung von Informationstechnologien nicht nur direkte Mehrwerte, die sich konkret monetär beziffern lassen, wie bspw. die Senkung von Unternehmensausgaben [9]. Vielmehr erlangen Unternehmen mit stärker ausgeprägten IT-Managementverfahren und einer intensiveren IT-Nutzung Wettbewerbsvorteile. Ein verbesserter Kundenservice kann zu einer höheren Leistung des Unternehmens und der Kundenkaufkraft führen. Direkt und sofort lässt sich der Mehrwert jedoch nicht monetär beziffern [10].

Vor diesem Hintergrund wird auch der unternehmerische Wert der Nutzung der Blockchain-Technologie betrachtet. Neben dem direkten, monetär messbaren Mehrwert, werden weitere indirekte Faktoren berücksichtigt. Dazu zählen bspw. die Steigerung der Kundenzufriedenheit und Datenqualität sowie das Ermöglichen neuer Angebote. Letztendlich kann der Mehrwert von Blockchain aufgrund der Architektur und Funktionsstruktur nicht separat für eine Organisation betrachtet werden. Es ist immer das gesamte Netzwerk zu berücksichtigen.[1] Gleichzeitig wird die Kombination der horizontalen und vertikalen Integration nach Coase ermöglicht. Organisationen eines geschäftlichen Netzwerkes sind innerhalb einer Blockchain horizontal integriert. Einzelne Daten und Transaktionen können jedoch zeitgleich mit definierten Teilnehmern oder ggf. nur unternehmensintern geteilt werden (vertikale Integration).

[1] Aufgrund der Natur der Blockchain, stellt diese Technologie ein Netzwerk, mit typischerweise mehreren Teilnehmern unterschiedlicher Organisationen dar, die Transaktionen über das gemeinsame Netzwerk austauschen und mittels einer verteilten Datenhaltung (Shared Ledger) speichern (vgl. Abschn. 5.2).

4.2 Mehrwerte von Blockchain in der Literatur

Mit dem verstärkten Interesse des Begriffes Blockchain, insbesondere der private permissioned Blockchain im geschäftlichen Umfeld, wird zunehmend diskutiert, inwiefern und in welcher Form Mehrwerte generiert werden und Unternehmen hiervon profitieren können. In vielen Literaturquellen ist mehrheitlich eine qualitative Argumentation anhand theoretischer Überlegungen vorzufinden. Oftmals fehlen ausreichende Praxiserfahrungen, um quantitativ fundierte Aussagen zu treffen [11, 12].

Eine umfassende Literaturanalyse zeigt auf, dass die Wissenschaft jedoch letztendlich auf einen gemeinsamen Bereich an Mehrwerten gekommen ist, von welchem die Unternehmen bei einer Einführung von Blockchain profitieren können. Auf dieser Basis lassen sich die folgenden sieben Dimensionen definieren:

I Verteilte Architektur ohne Intermediär Zentrale Systeme schaffen effiziente Regeln und Strukturen sowie Hierarchien in einem Netzwerk und vermeiden gleichzeitig die Doppelarbeit. Oft führt jedoch genau diese Zentralisierung zu hohen Kosten, die sich in Wirtschaftssystemen in Inflation, Korruption und Gewinnen widerspiegeln. Dezentralisierung ohne Intermediär spart diese Aufwände ein. Aufgrund des technologischen Fortschritts sinken die Kosten für verteilte Netzwerke zudem oftmals.[2] Gleichzeitig macht die Dezentralisierung das System robuster, flexibler, sicherer und effizienter [13]. Transaktionen werden nicht nur in nahezu Echtzeit verarbeitet und über alle Parteien bekannt, durch die Verringerung der Anzahl der Vermittler würden Kosten sinken und die Sicherheit verbessert (keine zentrale Instanz die über die Daten herrscht) [14]. Alle Netzwerkteilnehmer können Transaktionen lokal validieren, ohne sich auf eine externe Aufsichtsinstanz zu verlassen [15].

II Daten- und Manipulationssicherheit Die Datenblöcke der Blockchain sind im Nachhinein nicht mehr veränderbar. Die eingetragenen Informationen sind vor Manipulationen geschützt. Aufwendige Sicherungssysteme, wie oft bei zentralen

[2] *Moore's law* (Kosten für digitale Prozessoren halbieren sich alle 12 Monate); (2) *Kryder's Law* (Kosten für digitale Datenspeicherung z. B. Hard Drive Disk halbieren sich alle 18 Monate); (3) *Nielsen's Law* (Kosten für digitale Datenübertragung z. B. Bandbreite halbieren sich alle 21 Monate) [34].

Plattformen eingesetzt, sind in diesem Umfang meist nicht mehr erforderlich [16]. Insbesondere da, wo die nachweisliche Integrität von Daten eine Rolle spielt, trägt Blockchain zur Sicherung bei [15]. Nicht nur die Datenspeicherung, sondern auch die kryptografischen Konsensmechanismen ermöglichen zusätzlich sichere und manipulationsbeständige Abstimmungen, auch als Kryptodemokratie bezeichnet [13].

III Transparenz, Nachvollziehbarkeit und Konsens Der Shared Ledger garantiert einen gemeinsamen Konsens zwischen den Netzwerkteilnehmern. Transaktionen sind gleichzeitig transparent und nachvollziehbar [16]. Der gemeinsame Konsens ermöglicht nicht nur einen gemeinsamen Wissensstand im Netzwerk. Vielmehr können Transaktionen von allen Teilnehmern validiert sowie Identitäten oder Eigentumsrechte leicht verifiziert werden. Außerdem stimmen alle relevanten Netzwerkteilnehmer neuen Transaktionen zu (abhängig vom eingesetzten Konsens-Algorithmus), wodurch Netzwerkaktivitäten bzw. Geschäftsvorgänge automatisch überwacht werden [17]. Weiterhin führen transparente Verfahren und Transaktionen ebenfalls zu verändertem Verhalten von Einzelpersonen, als auch Organisationen. Potenziell könnten Betrugs- und Manipulationsraten von Verfahren damit abnehmen [18].

IV Kostenoptimierung und Zeitersparnis bei Transaktionen Transaktionszeiten für komplexe Interaktionen mit mehreren Parteien werden durch den Wegfall einer zentralen Prüfinstanz sowie durch digitale, automatisierte Prozessabläufe verkürzt. Gleichzeitig ergeben sich Kosteneinsparungen durch die Reduzierung von Vertrauensstellen sowie durch geringere Kommunikationsaufwände aufgrund des Shared Ledgers [17]. Neue Informationen stehen allen Teilnehmern gleichzeitig und in nahezu Echtzeit zur Verfügung [14]. Insgesamt nimmt die Flexibilität im Netzwerk zu, ist jedoch immer abhängig von der Anzahl der Transaktionen und der Größe des Netzwerkes [16].

V Automatisierung durch Smart Contracts Diese gelten als Verbesserung der allgemeinen Geschäftsfunktion, indem Management- und Kontrollprozesse automatisiert abgebildet werden können [14]. Smart Contracts wird weiterhin ein großes Optimierungspotenzial zugeordnet, weil sie vertrauenswürdige Dritte ersetzen [19]. Wird die Blockchain-Technologie als zwischen mehreren Parteien synchronisierte Datenschicht gesehen, können Smart Contracts als logische Schicht zur Steuerung und Überwachungen von Regularien gesehen werden [20].

VI Vertrauen Die Nachvollziehbarkeit und Verifizierung der Transaktionen schafft Vertrauen der Nutzer, insbesondere in Netzwerken, in denen die anderen Parteien einem nicht bekannt sind. Neue Handelsbeziehungen können sich ebenfalls ergeben [16]. Potenziell herrscht mehr Gleichheit, Gerechtigkeit und Freiheit für Organisationen in globalen Aktivitäten [21]. Hürden heutiger, meist regional beschränkter Regulierungssysteme, sind überwindbar. Lokalen Prüfern und Aufsichtsbehörden wird die Überprüfung der Regelkonformität einzelner Transaktionen erleichtert [17].

VII Verbesserte Audit- und Regulierungsfähigkeit Ist eine Überwachung durch Dritte (z. B. gesetzliche Vorgaben) erforderlich, reduziert Blockchain die Belastung des Regulierungssystems. Prüfern und Aufsichtsbehörden wird der Zugriff und die Nachvollziehbarkeit relevanter Transaktionsdetails erleichtert (ohne Eingriff dieser in den produktiven Betrieb) [17]. Zertifikate und Siegel, als z. B. Herkunftsnachweis von Bio- und Fair-Trade-Produkten, profitieren ebenfalls [20]. Ob sich auch die Anzahl der Manipulationsversuche in etablierten Prozessen senken lassen, ist bisher jedoch noch nicht belegt.

4.3 Bewertung des Mehrwertes von Blockchain am Praxisbeispiel

4.3.1 Der Bewertungsrahmen

Das Potenzial der Blockchain-Technologie für einen konkreten Anwendungsfall lässt sich durch die Gegenüberstellung des aktuellen Geschäftsnetzwerkes mit dem zukünftigen, auf Blockchain basierenden Netzwerkes ermitteln. Folgend wird der Bewertungsrahmen für die qualitative Mehrwertanalyse, auch als Wertschöpfungsanalyse bezeichnet, kurz erläutert. Ziel der qualitativen Wertschöpfungsanalyse ist es, den Mehrwert aus Sicht aller Beteiligten entlang der gesamten Wertschöpfungskette zu analysieren sowie die Geschäftsbeziehungen zwischen den beteiligten Stakeholdern abzubilden.

Die qualitative Mehrwertanalyse basiert auf dem von Czarnecki et al. entwickelten Bewertungsrahmen. Neben den klassischen Geld-, Güter- und Dienstleistungsströmen, werden auch Daten- und Informationsströme zwischen den verschiedenen Stakeholdern abgebildet [22]. In Abb. 4.2 ist exemplarisch ein Wirtschaftskreislauf zwischen zwei Stakeholdern dargestellt. Der aufgezeigte

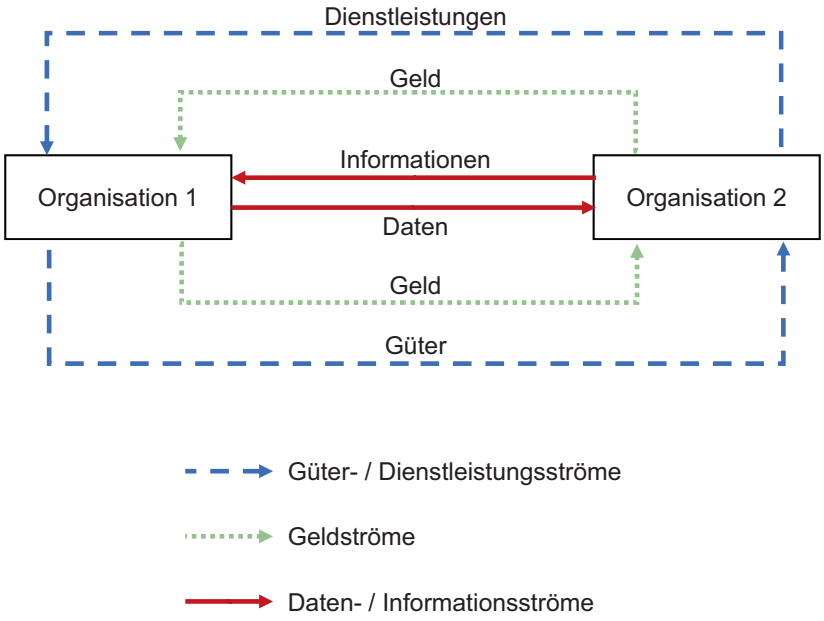

Abb. 4.2 Exemplarischer Bewertungsrahmen für die Analyse eines Wertschöpfungskreislaufs. (Eigene Darstellung in Anlehnung an Czarnecki et al. 2017, S. 188)

Daten- und Informationsfluss hat für die Betrachtung der Mehrwerte durch Blockchain eine besondere Bedeutung, da Daten und Informationen selbst über einen wirtschaftlichen Wert verfügen können. Weiterhin bilden Daten den Kernbaustein der Blockchain-Technologie.

Die Mehrwertanalyse auf Basis des aufgezeigten Bewertungsrahmens zielt nicht auf die Geschäftsmodelle der einzelnen Stakeholder ab, welche sich mit dem Business Model Canvas beschreiben ließen, sondern fokussiert primär den Wert für das Netzwerk bzw. Ökosystem zwischen den beteiligten Stakeholdern. Insbesondere für die Evaluierung des Mehrwertes von Blockchain ist es essenziell, nicht einzelne Netzwerkteilnehmer und deren Geschäftsmodelle zu betrachten, sondern primär das vollständige Ökosystem, in dem sich diese Stakeholder bewegen. Der Mehrwert ergibt sich grundlegend aus dem insgesamt veränderten Wirtschaftskreislauf. Deutlich wird dies bei der exemplarischen Betrachtung von zwei Anwendungsfälle im nachfolgenden Abschnitt.

4.3.2 Qualitativen Mehrwert manuell identifizieren

Der im vorherigen Abschnitt beschriebene Bewertungsrahmen dient in diesem Abschnitt als Basis für die manuelle, qualitative Mehrwertanalyse. Exemplarisch werden die folgenden beiden Anwendungsfälle betrachtet:

- Arztrezept für Medikamente für gesetzlich versicherte Patienten
- Bio-Siegel für Lebensmittel

Für beide Anwendungsfälle wird demonstriert, welcher Mehrwert für jeden einzelnen Stakeholder durch den Einsatz von Blockchain erzielt werden kann sowie die daraus resultierenden Änderungen im Ökosystem exemplarisch aufgezeigt.

4.3.2.1 Anwendungsfall 1: Arztrezept für Medikamente für gesetzlich versicherte Patienten

In der Diskussion geeigneter Anwendungsideen für Blockchain finden sich oft Prozesse bzw. Verfahren wieder, in denen eine Vielzahl von verschiedenen Teilnehmern am Austausch von Informationen beteiligt sind. Dabei kann oftmals keine zentrale Stelle im Netzwerk oder eine dem gesamten Netzwerk übergeordnete Organisation identifiziert werden. Demzufolge erfolgt der Informationsaustausch primär noch immer über dedizierte Schnittstellen oder auf Papierbasis, welches zumeist manuell weitergegeben wird. Digitale Standards sind in der Regel nur lokal zwischen einzelnen Teilnehmern vereinbart, haben aber keine netzwerkweite Wirkung.

Das elektronische Rezept, auch als eRezept bezeichnet, befindet sich in Deutschland derzeit in der Entwicklung und soll nach aktueller Information durch die Bundesregierung ab 2020 eingeführt werden [23]. Es existieren bereits diverse Pilotprojekte, die regional begrenzt durchgeführt werden und auf unterschiedlichen technischen Standards beruhen. Eine mögliche technische Implementierung könnte auf Basis der Blockchain-Technologie erfolgen, die im Folgenden näher betrachtet wird.

Gegenwärtiger Prozess Für die Verschreibung von Medikamenten existiert ein amtliches Formblatt, welches durch den aufgesuchten Arzt entsprechend ausgefüllt und in Papierform an den Patienten übergeben wird. Dieses Formblatt berechtigt den Patienten oder ggf. einen Stellvertreter für den Eintausch gegen das genannte Medikament in einer (Online)-Apotheke [24]. Bei Einlösung in einer Versandapotheke fällt i. d. R. zudem das Porto für den Rezeptversand an. Eine Möglichkeit zur Verifikation der Echtheit der Rezepte existiert gegenwärtig

nicht. Die Echtheit wird derzeit durch das Formblatt sowie durch Stempel und Unterschrift vom Arzt bestätigt, bietet aber Möglichkeiten zur Fälschung. Die Abrechnung der Medikamente zwischen der Apotheke und der gesetzlichen Krankenversicherung (GKV) erfolgt zumeist monats- oder quartalsweise in Form einer Sammelabrechnung. Dazu werden die Papierrezepte aufbewahrt und meist über einen Dienstleister, wie ein Apothekenrechenzentrum, gesammelt verarbeitet. Im Ergebnis hat die Apotheke ein finanzielles Delta zwischen Abgabe der Medikamente und Zahlungseingang durch die Krankenversicherung. Neben dem finanziellen Defizit, bildet sich weiterhin eine Informationsasymmetrie im Netzwerk aus, da unterschiedliche Netzwerkteilnehmer Informationen zu verschiedenen Zeitpunkten erhalten. Die Komplexität im Verfahren wird zusätzlich durch die hohe Anzahl individueller Netzwerkakteure verstärkt. Gegenwärtig existieren in Deutschland rund 19.000 Apotheken, [25] 72.000 Arztpraxen [26] und 109 GKV, die circa 72 Mio. Patienten versichern [27]. Die privaten Krankenversicherungen (PKV) sind in dem Fallbeispiel nicht betrachtet, da sich der Abrechnungsprozesse zwischen GKV und PKV stark unterscheidet.

Der gegenwärtige Wertschöpfungskreis ist in Abb. 4.3 gemäß dem oben dokumentierten Prozess dargestellt.

Potenzieller Prozess auf Basis der Blockchain Der Einsatz einer Blockchain könnte den in Abb. 4.4 dargestellt Kreislauf ergeben. Es sei darauf hingewiesen,

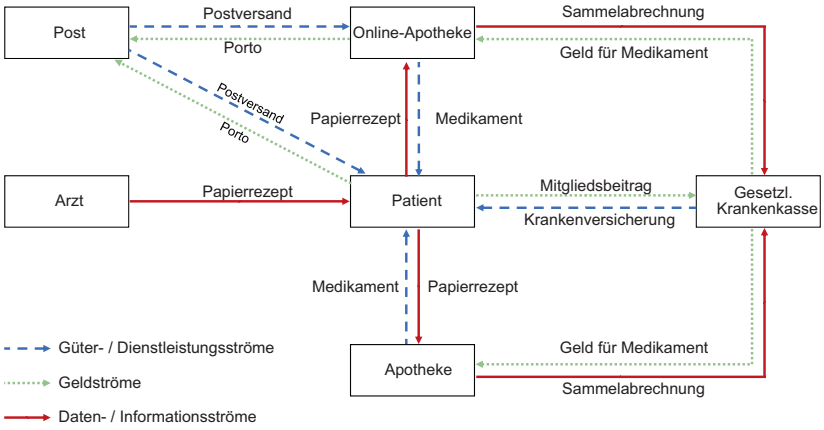

Abb. 4.3 Bewertungsrahmen für den Anwendungsfall „Arztrezept" – Heute. (Eigene Darstellung)

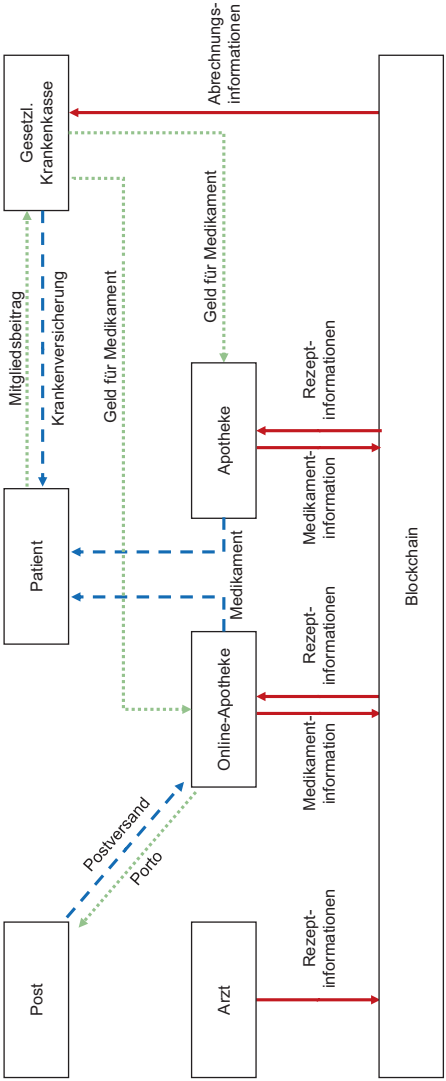

Abb. 4.4 Bewertungsrahmen für den Anwendungsfall „Arztrezept" – mit Blockchain. (Eigene Darstellung)

dass die Blockchain nicht als zentrale Komponente, sondern als zwischen allen Beteiligten verteiltes Netzwerk zu sehen ist.[3]

Auf Basis der Blockchain würden Verordnungen für Medikamente vom Arzt als Datensatz im Zuge einer Transaktion im Ledger gespeichert. Eine Dokumentation auf Papier erfolgt nicht mehr. Im nächsten Schritt entscheidet der Patient in welcher Apotheke er die Verordnung einlösen möchte und gibt ggf. die Information für diese Apotheke frei. Wird der Patient erfolgreich mithilfe der Blockchain authentifiziert, händigt die Apotheke das verordnete Medikament aus. Der GKV, ebenfalls Teilnehmer im Blockchain-Netzwerk, wird das Medikament automatisch in Rechnung gestellt. Eine explizit erstellte Rechnung könnte entfallen. Der Patient kann über seine GKV Zugriff auf die Blockchain erhalten, ohne selbst einen physischen Netzwerkknoten zu betreiben (passiver Netzwerkteilnehmer). Der Zugang ist über bestehende Apps oder Portale der GKV denkbar. Würde anstatt einer Blockchain als verteiltes Netzwerk, eine Plattform als zentrale Komponente genutzt werden, benötigt das Ökosystem eine zusätzliche zentrale organisatorische Instanz als Besitzer und Betreiber dieser Plattform. Diese organisatorische Instanz wäre mit zusätzlichen Geldströmen für die Hardware und Administration verbunden und würde den erzielbaren Mehrwert des Lösungskonzeptes verringern. Weiterhin sind alle Netzwerkteilnehmer gezwungen, dieser Instanz vertrauen. Im dargestellten Kreislauf wird für den Betrieb der Blockchain-Knoten ggf. zusätzlich ein IT-Provider eingebunden, der sich jedoch analog zu bereits heute eingesetzter IT-Provider verhält (vgl. Apothekenrechenzentrum, IT-Ausrüstung und Betrieb für Arztpraxen, Rechenzentrum der GKV).

Der Mehrwert durch den Einsatz von Blockchain Zusammenfassend zeigen sich für alle Beteiligten Potenziale, die administrativen Aufwände zu verringern sowie Prozesse patientenorientiert zu gestalten (digitaler Prozess ohne Papier). Ebenfalls ließen sich die vielen 1:1 Beziehungen zwischen Netzwerkakteuren reduzieren, die sich im GKV-Kontext heute als problematisch erweisen. Zusätzlich könnten Intermediäre, z. B. in Form von Abrechnungszentren, eingespart und Prozesse effizienter und schneller gestaltet werden. Beim Onlinehandel (z. B. Online-Apotheken) führt diese sichere Datenübermittlung zusätzlich zur Reduzierung der Transaktionszeiten. Der Zeitverlust, bedingt durch

[3]Jeder Kasten in der Abbildung repräsentiert lediglich eine Komponente des Ökosystems, wobei jede Komponente in der realen Umgebung in mehrfacher Ausprägung vorhanden sein kann.

das Einsenden des Papierrezeptes zur Online-Apotheke, entfällt gänzlich. Ein zusätzlicher Mehrwert der Blockchain ergibt sich durch eine transparente Nachvollziehbarkeit, indem das mehrfache Einlösen eines Rezeptes verhindert wird [16] (Analog zum Double-Spending Problem). Der Einsatz der Blockchain könnte einen jährlichen finanziellen Schaden zwischen 680 Mio. und 2,72 Mrd. EUR im Gesundheitswesen abwenden, welcher laut Transparency Deutschland jährlich durch Rezeptbetrug allein in Deutschland entsteht [28]. Zuletzt kann der Versicherte zudem von einer automatischen und digitalen Zuzahlungsbefreiung profitieren. Ist der Patient bspw. pauschal durch die Krankenversicherung von der Zuzahlung befreit, kann dies als Status in der Blockchain für den Patienten hinterlegt und durch die Apotheke abgefragt werden. Außerdem ließe sich mit Hilfe von Smart Contracts ermitteln, in welcher Höhe der einzelne Versicherte im laufenden Jahr bereits Zuzahlungen geleistet hat. Übersteigen diese die Belastungsgrenze (2 % des Familien-Bruttoeinkommens eines Jahres) [29] kann der Smart Contract den Status in der Blockchain automatisch hinterlegen. Das Bruttoeinkommen kann mit einem Orakel im System der Krankenkasse abgefragt werden, ohne diese Informationen in der Blockchain zu hinterlegen. Die manuelle Beantragung der Zuzahlungsbefreiung bzw. das Mitführen eines Nachweises durch den Patienten über die Befreiung von Zuzahlungen wären nicht mehr notwendig.

Zusammenfassend unterscheidet sich die Blockchain-Version des Ökosystems von dem gegenwärtigen Kreislauf in folgenden Aspekten:

- Daten- und Informationsströme werden digital und gebündelt über die Blockchain abgebildet. Bisher findet der überwiegende Datenaustausch im Netzwerk auf Papier statt, der mit der Blockchain vollständig entfällt. Der Informations- und Kommunikationsfluss wird somit beschleunigt.
- Die Kommunikation erfolgt über ein Netzwerk mit einer standardisierten Schnittstelle, individuelle Schnittstellen zwischen verschiedenen Netzwerkteilnehmern entfallen. Das senkt die Kosten und die Komplexität für den Betrieb existierender Schnittstellen sowie wird die Anzahl von Angriffspunkten und Fehlerquellen reduziert.
- Portogebühren sowie Transaktionszeiten durch den Postversand entfallen.
- Informationsasymmetrien wird durch einheitliche Datenströme entgegengewirkt.
- Die Datenqualität wird durch die digitale Abbildung und Weitergabe der Informationen erhöht, wobei alle Eingaben und Transaktionen fortlaufend, automatisch validiert und geprüft werden.
- Der Patient wird im Prozess entlastet, da kein Versand bzw. keine manuelle Weitergabe von Unterlagen notwendig ist.

- Die Apotheke wird im Prozess entlastet, da keine manuelle Aufbewahrung und Abrechnung der Papierrezepte mehr erfolgt. Weiterhin kann die Abrechnung mit der Krankenversicherung schneller erfolgen und das finanzielle Delta gesenkt werden.
- Online-Apotheken werden attraktiver, da die Medikamente durch den Entfall des Rezeptversands früher beim Patienten eintreffen.
- Ggf. wird ein IT-Provider eingebunden (kann auch durch interne IT der Teilnehmer abgebildet werden).

4.3.2.2 Anwendungsfall 2: Bio-Siegel für Lebensmittel

Für die Nachverfolgung von Lieferketten, insbesondere, wenn Nachweise zur Herkunft einzelner Waren zu erbringen sind, wird Blockchain oftmals als die optimale Lösung genannt. Sollen weiterhin Identitätsnachweise in Form von Siegeln (z. B. Bio- oder Steuersiegel) oder Zertifikaten (z. B. Herstellernachweis für Ersatzteile oder Zollsiegel) erbracht werden, ist dies gegenwärtig mit komplexen administrativen Prozessen verbunden, da der länder- und organisationsübergreifende Datenaustausch nicht standardisiert ist. Fälschungen oder Ungenauigkeiten in der Dokumentation (z. B. Begleitdokumente für die Ware) lassen sich nur schwer verhindern oder erkennen. Für den Endverbraucher bietet sich i. d. R. keine Möglichkeit die Herkunft der Waren oder das Siegel sicher zu verifizieren, da ihm die Informationen bzw. begleitenden Dokumente nicht vorliegen. Oftmals gilt dies jedoch auch für Organisationen innerhalb der Lieferkette. Auch diese vertrauen auf die Korrektheit der Produktangaben in den Begleitdokumenten, da auch weiterverarbeitende Betriebe zumeist keine Möglichkeit besitzen, Bio-Angaben der Lieferanten sicher nachzuprüfen bzw. die Herstellung der Ausgangsprodukte zweifelsfrei nachzuvollziehen.

Exemplarisch für dieses Anwendungsgebiet wird nachfolgend der Prozess zur Vergabe und Verifizierung von Bio-Siegeln für Lebensmittel betrachtet. Bio-Siegel erfreuen sich einer stark steigenden Beliebtheit bei den Konsumenten. Der Umsatz mit Bioprodukten steigt in Deutschland im Schnitt um rund 5 % pro Jahr, [30] wobei die Anzahl an Bio-Produkten in den Regalen der Einzelhändler um jährlich rund 2 % steigt [31].

Gegenwärtiger Prozess Für Bio-Produkte gelten gegenwärtig keine übergreifenden Standards. Vielmehr sind diese abhängig vom konkreten Siegel bzgl. der dahinterstehenden Organisation, die für die Vergabe der Siegel und Prüfung der Betriebe verantwortlich ist. Die jeweilige Biosiegel-Kontrollstelle prüft die Betriebe anhand festgelegter Kriterien in festen Abständen. Dabei werden nicht einzelne Produkte, sondern der Betrieb und die Verarbeitung insgesamt zertifiziert und der Betrieb somit berechtigt, bei erfolgreicher Prüfung, das Bio-Siegel für die einzelnen Produkte zu verwenden. Neben einer schriftlichen Zertifizierung des

Betriebs, können die einzelnen Produkte mit papierbasierten Siegeln versehen werden (z. B. Bio-Aufkleber). Die Kriterien für die Siegelvergabe sind zumeist auf der Webseite der Anbieter, auch für Konsumenten, transparent einsehbar. Doch besteht für den Endverbraucher und meistens auch für die verarbeitenden Betriebe innerhalb der Lieferkette keine Möglichkeit, zu überprüfen, ob das jeweilige Produkt tatsächlich von dem Bio-Zertifizierten Lebensmittelerzeuger stammt. Vielmehr steht das Vertrauen zwischen den Parteien im Vordergrund. Vereinfacht lässt sich die Wertschöpfungskette des heutigen Prozesses demnach wie in Abb. 4.5 dargestellt beschreiben.

Potenzieller Prozess auf Basis der Blockchain Mit dem Einsatz der Blockchain-Technologie ließe sich der in Abb. 4.6 dargestellte Wirtschaftskreislauf realisieren. Wie bereits auch im vorherigen Anwendungsfall sei darauf hingewiesen, dass die Blockchain nicht als zentrale Komponente, sondern als zwischen allen Beteiligten verteiltes Netzwerk zu sehen ist.[4]

Die bisher papierbasierten Siegel und Zertifikate lassen sich digital über die Blockchain abbilden, indem die mit den Siegeln verbundenen Informationen direkt und für alle Teilnehmer transparent in der Blockchain gespeichert werden. Für jedes Tier des Lebensmittelerzeugers, als auch für jedes fertige Produkt des Lebensmittelherstellers wird ein Digital Twin[5] in der Blockchain erstellt. Da die Transaktionen und die darin enthaltenden Daten in den Blöcken unveränderbar abgespeichert sind, sind die Informationen gleichzeitig vor Manipulationen oder Datenverlusten geschützt. Die Verlinkung zwischen dem Digital Twin und dem physischen Produkt lässt sich über mehrere Wege sicherstellen. Produkte können mittels QR-Codes oder RFID-Chips identifiziert und in der Blockchain gesucht werden. Derartige Aufkleber oder Chips können zusätzlich mit einem Schutz gegen Kopie (z. B. für RFID Chips) oder einem Schutz gegen Wiederverwendung ausgestattet werden. Um weiterhin sicherzustellen, dass das initial in der Blockchain registrierte Ausgangsprodukt mit dem Endprodukt beim

[4]Jeder Kasten in der Abbildung repräsentiert lediglich eine Komponente des Ökosystems, wobei jede Komponente in der realen Umgebung in mehrfacher Ausprägung vorhanden sein kann.

[5]Ein digital twin (deutsch: Digitaler Zwilling) ist das digitale Abbild eines materiellen oder immateriellen Gutes oder Prozesses aus der realen Welt. Der digital twin ermöglicht einen übergreifenden Datenaustausch und bildet die Daten des Zwillings aus der realen Welt ab. Insbesondere für die Dokumentation verschiedener Stati, die Simulation von Prozessen oder das Anbieten von Diensten werden diese oftmals eingesetzt.

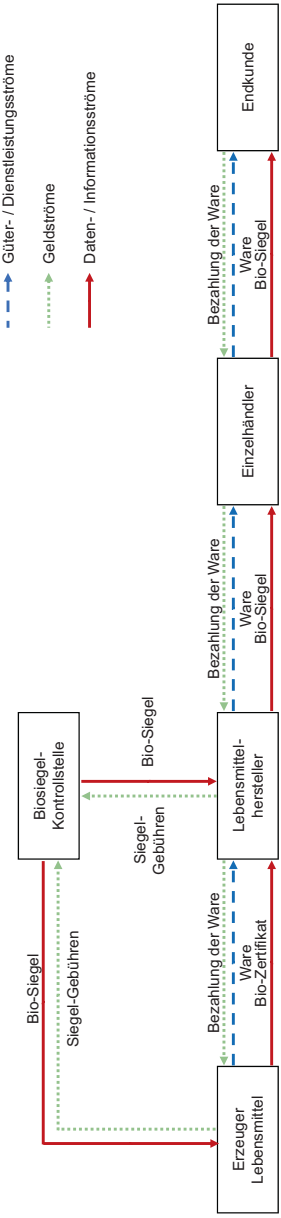

Abb. 4.5 Bewertungsrahmen für den Anwendungsfall „Bio-Siegel" – Heute. (Eigene Darstellung)

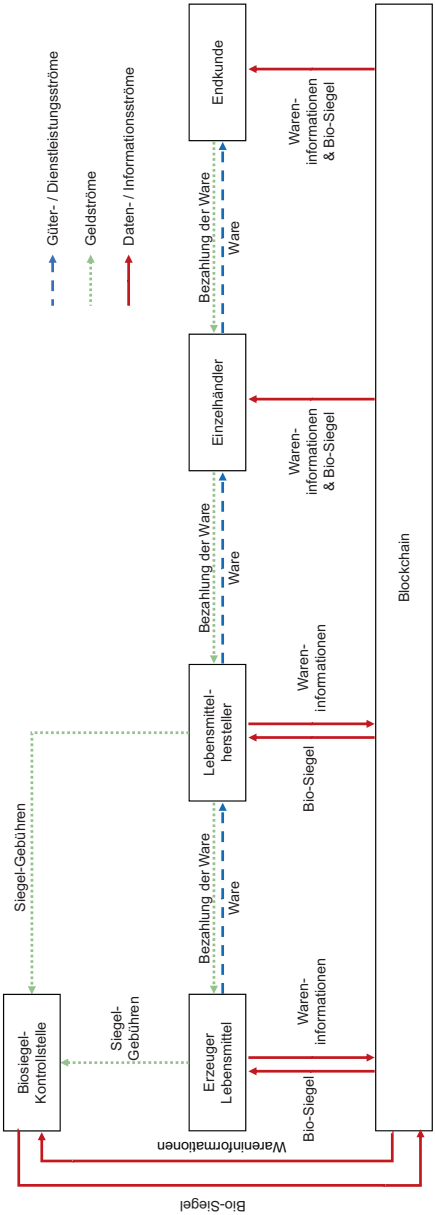

Abb. 4.6 Bewertungsrahmen für den Anwendungsfall „Bio-Siegel" – mit Blockchain. (Eigene Darstellung)

Konsumenten übereinstimmt, kann bereits zu Beginn die DNA der Tiere oder Laborergebnisse der Lebensmitteluntersuchung in der Blockchain registriert werden. Diese wirken als eindeutiger Fingerabdruck für das konkrete Produkt. Verifiziert werden können diese Informationen stichprobenartig durch eine Lebensmittelbehörde oder die Biosiegel-Kontrollstelle, indem bspw. DNA-Proben fertiger Fleischerzeugnisse mit den in der Blockchain abgespeicherten DNA-Proben der Ausgangsprodukte abgeglichen werden.

Der Mehrwert durch den Einsatz von Blockchain Zusammenfassend profitiert das Ökosystem in folgenden Aspekten:

- Siegel sind bis zum Endkunden verifizierbar sowie vor Manipulation geschützt. Das stärkt das Vertrauen in die Siegel und die Lebensmittelindustrie und kann für diese zusätzliches Geschäft generieren.
- Informationen werden für alle Netzwerkteilnehmer transparent und sind in nahezu Echtzeit verfügbar.
- Senkung der administrativen Aufwände für die Siegelvergabe, Weitergabe und Kontrolle.
- Die Kommunikation und Datenweitergabe sind digital über ein Netzwerk abgebildet, welches zudem eine standardisierte Schnittstelle zwischen allen Netzwerkteilnehmern schafft.
- Informationsasymmetrien wird durch einheitliche Datenströme entgegengewirkt.
- Endprodukte einzelner Ausgangsprodukte lassen sich leichter bestimmen. Der Rückruf bestimmter Waren lässt sich effizient gestalten, wenn bekannt ist, welche Endprodukte wann und wo verkauft bzw. weitergeben wurden. Massenrückrufaktionen für ganze Monatsproduktionen könnten somit verhindert werden.
- Die Qualität der Endprodukte wird erhöht, indem das Einbringen nicht zertifizierter Waren erschwert wird. Bei ausreichender Verbreitung kann Lebensmittelskandalen, die z. T. gesundheitlich bedenkliche Auswirkungen mit sich bringen, vorgebeugt werden.
- Ggf. wird ein IT-Provider eingebunden (kann auch durch interne IT der Teilnehmer abgebildet werden).

4.3.3 Fazit der manuellen Bewertung

Die manuelle Bewertung hat gezeigt, dass es sinnvoll ist, die einzelnen Wertströme sowie Netzwerkteilnehmer separat zu betrachten, um den qualitativen

Mehrwert zu bestimmen sowie die einzelnen Mehrwertbereiche gezielt voneinander abzugrenzen. Die Gegenüberstellung der heutigen und potenziell zukünftigen, auf Blockchain basierenden Wertschöpfungskette ermöglicht zudem die Ermittlung des Deltas zwischen beiden Varianten bezüglich der finanziellen, produktbezogenen und datentechnischen Aspekte. Ergänzend lassen sich daraus Änderungen in den (Prozess-)Aufwänden der einzelnen Teilnehmer ableiten, welche für die Erzeugung einzelner Ströme notwendig sind.

Hieraus lässt sich ableiten, dass sich durch den Einsatz von Blockchain ein potenzieller Mehrwert für das gesamte Ökosystem sowie für jeden einzelnen Teilnehmer ergibt. Ein monetärer Mehrwert entsteht, wenn die Reduzierung der Versand-, Prozess- und Datenaufbereitungskosten im Vergleich zu den Kosten für den Betrieb der Blockchain höher ausfallen. Zusätzlich entfallen Mehraufwände bzw. Fehler aufgrund schlechter oder unzureichender Datenqualität durch z. B. Medien- und Systembrüche. In Bezug auf Dienstleistungsaspekte liegt der Mehrwert vorrangig bei den Versicherten bzw. den Endkunden. Im Sinne kundenorientierter Prozesse werden diese entlastet und erhalten gleichzeitig einen zusätzlichen Nutzen (z. B. Transparente Validierung der Bio-Siegel), der sich in den weichen betriebswirtschaftlichen Faktoren (soft Facts) widerspiegelt. Diese lassen sich nicht in betriebswirtschaftlichen Kennzahlen (wie z. B. Kosten, Kapitalumschlag, etc.) abbilden, beeinflussen jedoch die Handlungsweisen sowie die Entscheidungen der Kunden (z. B. Zufriedenheit, Weiterempfehlung, Kundentreue, etc.) [32]. Daraus abgeleitet bilden Blockchain-Anwendungen zunehmend Value Cases anstatt klassischer Business Cases ab. Weiterhin liegen die Daten mithilfe der Blockchain generell digital und in einer höheren Datenqualität vor. Tipp- und Lesefehler im Papierprozess entfallen. Zusätzlich sind alle Transaktionen geprüft, die Daten validiert und manipulationssicher gespeichert sowie in nahezu Echtzeit verfügbar. Auf dieser Basis lassen sich zudem vorhandene manuelle Verarbeitungsprozesse durch Smart Contracts automatisieren.

In Summe ergeben sich durch den Einsatz der Blockchain-Technologie neben klassischen Einspar- und Optimierungspotenzialen, gleichzeitig neue Angebote, die wiederum zusätzliche Erträge erzielen können.

4.4 Indikationsmodell zur Identifizierung des qualitativen Mehrwertes

Wie am praktischen Anwendungsfall aufgezeigt, ist eine Analyse der qualitativen Mehrwertaspekte anhand des Bewertungsrahmens aus Abschn. 4.3.1 für ein individuelles Ergebnis durchaus zielführend. Für eine erste Indikation der potenziellen Mehrwerte jedoch gleichzeitig sehr aufwändig.

Auf Grundlage der allgemeinen Mehrwerte von Blockchain (Abschn. 4.2) sowie der Betrachtung der Wertschöpfungsströme (Abschn. 4.3.2) stellt nachfolgendes Kapitel ein Modell vor, aus dem sich potenzielle Mehrwertaspekte für einen konkreten Anwendungsfall systematisch identifizieren und bewerten lassen. Ziel dieses Modells ist es, dem Anwender einen effizienten und gut wiederverwendbaren Weg zu bieten, die qualitativen Mehrwertaspekte für einen konkreten Anwendungsfall gut überschaubar zu ermitteln.

4.4.1 Die Nutzwertanalyse als Modellbasis

Um komplexe Handlungsalternativen vollständig zu erfassen sowie mehrdimensional zu bewerten, eignet sich die Nutzwertanalyse. Hierzu wird jede Handlungsalternative bzw. Problemstellung mittels definierter Bewertungskriterien in unterschiedliche Teilaspekte segmentiert und einzeln bewertet. Den Kriterien können quantitative sowie qualitative Merkmale zugrunde liegen (z. B. technische, finanzielle oder soziale Aspekte). Zusätzlich sind die einzelnen Kriterien auf Basis ihres Einflusses bzw. der Auswirkung auf die übergreifende Problemstellung nach gewichtet. In Summe ergeben die Einzelgewichtungen 100 % bzw. 1. Die Gewichtung der Kriterien sowie die gewichtete Punktzahl der Entscheidungsalternativen führt zu einer objektiven Vergleichbarkeit der unterschiedlichen Optionen. Im Besonderen eignet sich die Nutzwerkanalyse für die Bewertung von Handlungsoptionen, die nicht ausschließlich zahlenbasiert (z. B. anhand finanzieller Kenngrößen) erfolgen kann [33].

Zum besseren Verständnis der Nutzwertanalyse, ist in Tab. 4.1 als Beispiel die Bewertung von zwei Handlungsoptionen anhand definierter Kriterien dargestellt. Für die Bewertung können je Kriterium 1 (schlecht) bis 4 (sehr gut) Punkte vergeben werden.

Tab. 4.1 Beispiel einer Nutzwertanalyse

Kriterien	Gewichtung	Option A		Option B	
		Punkte	gewichtet	Punkte	gewichtet
Kosten	0,2 / 20 %	4	0,8	3	0,6
Qualität	0,3 / 30 %	2	0,6	4	1,2
Innovationsgrad	0,25 / 25 %	3	0,75	2	0,5
Nachhaltigkeit	0,15 / 15 %	2	0,3	3	0,45
Service	0,1 / 10 %	4	0,4	2	0,2
SUMME	**1 / 100 %**	**15**	**2,85**	**14**	**2,95**

Dieses Beispiel zeigt zugleich auf, dass die Gewichtung für die korrekte Bewertung der Optionen essentiell ist. In dem Beispiel (Tab. 4.1) erreicht *Option A* zwar absolut die höhere Punktanzahl, doch ist *Option B* für die eigentliche Problemstellung (in der Nutzwerkanalyse anhand der Gewichtung widergespiegelt) besser geeignet. Option B erreicht gewichtet 0,1 mehr Punkte.

4.4.2 Das Mehrwert-Indikationsmodell

Ist ein potenzieller Anwendungsfall für Blockchain identifiziert, bleibt zu klären, warum Blockchain eingesetzt werden sollte und wo direkt der Mehrwert für jede integrierte Organisation sowie das gesamte Netzwerk liegt. Zur Evaluierung und Bewertung des qualitativen Mehrwertes dient das Indikationsmodell.

Auf Basis der Literaturanalyse konnten die folgende Mehrwertaspekte der Blockchain-Technologie extrahiert werden (vgl. Abschn. 4.2):

- Verteilte Architektur ohne Intermediär
- Daten- und Manipulationssicherheit
- Transparenz, Nachvollziehbarkeit und Konsens
- Kostenoptimierung und Zeitersparnis bei Transaktionen
- Automatisierung durch Smart Contracts
- Vertrauen
- Verbesserte Audit- und Regulierungsfähigkeit

Folgende Aspekte zu möglichen Mehrwerten wurden zudem in den Praxisbeispielen zum eRezept (Abschn. 4.3.2.1) und zu den digitalen Bio-Siegeln (Abschn. 4.3.2.2) aufgezeigt:

- Entfall von Intermediären, welche Prozesse verzögern und die Kosten steigern und damit Reduzierung der Prozessdurchlaufzeiten.
- Reduzierung des administrativen und Kommunikationsaufwands.
- Abbau der vielen 1:1 Verbindungen und Insellösungen, die Prozesse ineffizient machen und eine ganzheitliche Sicht auf die Daten verhindern sowie zu höheren Aufwänden für den Betrieb und Sicherung der Schnittstellen führen.
- Reduzierung der Informationsasymmetrie durch Erhöhung der Transparenz.
- Abbau von Misstrauen im Netzwerk (Versicherer gegenüber den Versicherten und Konsumenten gegenüber den Lebensmittelherstellern).

- Unterbindung von Manipulationen und möglichem Betrug bei z. B. der Abrechnung sowie Reduzierung der hieraus resultierenden Verluste.
- Erhöhung der Datenqualität (Medienbruch wird vermieden und Eingaben werden durch Smart Contracts validiert). Schaffung der Datengrundlage für bessere und zuverlässigere Entscheidungen.
- Automatisierung (z. B. von Prozessen) durch Smart Contracts.
- Neue Serviceangebote und kundenorientierte Prozesse durch Automatisierung, Datenkonsolidierung und Transparenz/gemeinsamen Konsens.

Zur Ermittlung der grundsätzlichen Vorteile der Blockchain in einem konkreten Anwendungsfall sowie für eine erste Indikation zum Umfang des Mehrwertes dient das Indikationsmodell (Tab. 4.2).

Die Basiskomponente des Indikationsmodells bildet die Nutzwertanalyse (vgl. Abschn. 4.4.1). Die verschiedenen Mehrwertaspekte sind als Kriterien mit unterschiedlichen Ausprägungswerten dargestellt. Die Mehrwertaspekte (Kriterien) repräsentieren die Bereiche, in denen Blockchain für den konkreten Anwendungsfall grundsätzlich einen Mehrwert erzeugen kann. Zu jedem Mehrwertaspekt ist vom Nutzer der Ausprägungsgrad, welcher die heutige Situation des Anwendungsfalls ohne Einsatz der Blockchain am ehesten beschreibt, zu wählen. Die Kurzbeschreibungen helfen dem Anwender bei der Punktevergabe für die einzelnen Kriterien, indem die Bedeutung der Punkte eins bis vier jeweils klar beschrieben sind. Diese Ausprägungen definieren exakt die Problemsegmente, welche die einzelnen Mehrwertaspekte der Blockchain adressieren. Zudem sind die Ausprägungen entsprechend ihrem potenziellen Mehrwert nach geordnet. Bei jeder Ausprägung im Indikationsmodell steigt der qualitative Mehrwert für diesen Aspekt nach rechts hin. Die Summe der gewählten Ausprägungen gibt Aufschluss darüber, in welchem Segment welcher Mehrwert zu erwarten ist. Das Ergebnis des Indikationsmodells zeigt demnach die Summe der möglichen Mehrwerte auf sowie welche Defizite der gegenwärtigen Situation ggf. abgestellt werden können. Weiterhin ermöglicht die gewichtete Punktzahl den Vergleich verschiedener Anwendungsideen mit einem Fokus auf bestimmte Schwerpunkte (Dargestellt durch die Gewichtungen). Im Indikationsmodell ist die Gewichtung auf Basis üblicher Einsatzgebiete sowie Anforderungen aus der Wirtschaft vorbelegt. Diese können jedoch an individuelle Bedürfnisse einer Organisation angepasst werden. Hierbei ist jedoch zu beachten, dass alle Bewertungen verschiedener Anwendungsideen mit der gleichen Gewichtung durchgeführt werden,

um die Vergleichbarkeit der Ergebnisse zu gewährleisten. Das vollständige Modell, inklusive der exemplarischen Anwendung, ist in Abschn. 4.4.3 zu finden.

4.4.3 Anwendung des Modells im Praxisbeispiel Bio-Siegel

Hinsichtlich der qualitativen Mehrwertanalyse stellt das Indikationsmodell (Tab. 4.2) einen generischen Ansatz dar. Die Anwendung wird in diesem Abschnitt anhand des Praxisbeispiels Bio-Siegel für Lebensmittel exemplarisch aufgezeigt. Auf Basis der heutigen Prozessabläufe sowie der fachlichen Zielsetzungen lassen sich die einzelnen Ausprägungen jeder Kategorie für diesen Anwendungsfall exemplarisch wie im Indikationsmodell abgebildet darstellen (Tab. 4.2).

Ebenso lassen sich die Ergebnisse des Indikationsmodells grafisch in einem Spinnendiagramm darstellen (Abb. 4.7). Hier wird deutlich erkennbar, dass Blockchain in diesem konkreten Anwendungsfall vorrangig einen Mehrwert durch das Schaffen der Manipulationssicherheit bietet, indem feste Vertrauensstrukturen im Ökosystem etabliert werden. Ebenso ergeben sich große Potenziale durch die Reduzierung der Transaktionszeiten und Verbesserung der Transaktionsverarbeitung sowie durch Standardisierung der Kommunikationsstrukturen. Die Kommunikationsstränge werden konsolidiert bzw. über nur ein Netzwerk abgebildet, wobei Intermediäre trotz Reduzierung der organisationseigenen Transaktionsaufwände sowie Reduzierung der Kommunikationskanäle nicht etabliert werden. Insgesamt ist das Ergebnis des Indikationsmodells mit dem anhand des Bewertungsrahmens identifizierten Resultats vergleichbar. Der Vorteil des Indikationsmodells besteht jedoch darin, dass es die qualitativen Mehrwertaspekte beschreibt und gleichzeitig generisch, ohne größeren Aufwand, auf weitere beliebige Anwendungsfälle übertragbar ist. Für jeden Anwendungsfall eigens einen individuellen Bewertungsrahmen des Wertschöpfungskreislaufes zur Identifizierung möglicher Mehrwerte durch eine Blockchain zu generieren, wäre unverhältnismäßig aufwändiger. Zusätzlich lässt sich das Mehrwertpotenzial mehrerer Anwendungsideen einfach über die Summe der gewichteten Punkte, im Fall der Bio-Siegel 3,21, vergleichen. Wichtig ist dabei zu beachten, dass alle Bewertungen mit der gleichen Verteilung der Gewichtungen vorgenommen werden.

Tab. 4.2 Indikationsmodell zur Evaluierung qualitativer Mehrwertaspekte. Exemplarische Anwendung auf den vorgestellten Anwendungsfall „Bio-Siegel für Lebensmittel."

Mehrwertaspekte	Gewichtung	Ausprägung der heutigen Gegenwart - potenzieller Mehrwertbeitrag durch Blockchain & Punkte				Punkte/ gewichtet
		gering			hoch	
		1	2	3	4	
Intermediäre	0,15 / 15 %	Prozess läuft ohne direkten Intermediär, indem gemeinsame Netzwerk-strukturen genutzt werden	Zur Bündelung und Verifikation der Transaktionen sind einige Intermediäre eingebunden, die zu Ineffizienzen führen	Im Prozess sind eine Vielzahl von Intermediären eingebunden, die Kosten verursachen, Prozesse verlangsamen und Intransparenzen schaffen	Analoge oder 1:1 Kommunikations-strukturen erfordern heute keine Intermediäre, erzeugen jedoch hohe Aufwände	4 / 0,6
Transparenz & Nachvollziehbarkeit	0,12 / 12 %	Prozesse sind heute vollständig transparent und nachvollziehbar	Prozesse sind transparent, jedoch nicht alle Daten nachvollziehbar (z. B. Transaktionsreihenfolge unsauber dokumentiert)	Aus historischen/ organisatorischen Gründen sind Prozesse weder transparent noch nachvollziehbar, was teils zu Dokumentationslücken führt	Teils werden künstliche Intransparenzen geschaffen, um Vorteile für die eigene Organisation zu erzielen, Stati/Besitzverhältnisse sind nicht nachvollziehbar	3 / 0,36

(Fortsetzung)

Tab. 4.2 (Fortsetzung)

Mehrwertaspekte	Gewichtung	Ausprägung der heutigen Gegenwart - potenzieller Mehrwertbeitrag durch Blockchain & Punkte				Punkte/ gewichtet
		gering			hoch	
		1	2	3	4	
Konsens	0,07 / 7 %	Im Netzwerk haben alle Teilnehmer eines Geschäftsvorgangs stets den gleichen Informationsstand	Der Informationsabgleich im Geschäftsvorgang erfolgt zeitlich verzögert, was ggf. Prozesse verlangsamt, jedoch keine weiteren negativen Folgen hat	Unterschiedliche Informationsstände (Insellösungen) führen zu Missverständnissen und falschen Entscheidungen im Geschäftsprozess	Unterschiedliche Informationsstände werden teils gezielt durch einzelne Teilnehmer zu deren Vorteil genutzt	3 / 0,21
Transaktionszeiten und -verarbeitung	0,05 / 5 %	Transaktionsprozesse sind automatisiert, daher nur geringe Wartezeiten	Dedizierte Synchronisierungs- und Austauschmechanismen im Netzwerk erhöhen die Prozessdurchlaufzeit im Vergleich zur Bearbeitungszeit	Manuelle Bearbeitungsschritte verlangsamen die digitale Verarbeitung und führen zu hohen Wartezeiten sowie Fehleranfälligkeit	Analoge Kommunikationswege (z. B. Post) erhöhen die Prozessdurchlaufzeit stark, wobei Medien- und Systembrüche zusätzliche Ineffizienzen verursachen	3 / 0,15

(Fortsetzung)

Tab. 4.2 (Fortsetzung)

Mehrwertaspekte	Gewichtung	Ausprägung der heutigen Gegenwart - potenzieller Mehrwertbeitrag durch Blockchain & Punkte				Punkte/ gewichtet
		gering			hoch	
		1	2	3	4	
Kommunikations-kanäle	0,05 / 5 %	Vollständig digitale Kommunikation die gebündelt über wenige Schnittstellen zu den Partnern erfolgt	Digitale Kommunikation, wobei viele individuelle Verbindungen zwischen Partnern implementiert sind	Teildigitalisierte Kommunikation, wobei unterschiedliche Kanäle je Partner genutzt werden (viele 1:1 Verbindungen)	Einbindung analoger Kommunikations-kanäle (z. B. Post), die zusätzliche Kosten verursachen und Kommunikationswege verlangsamen	3 / 0,15
Manipulations-sicherheit	0,18 / 18 %	Transaktions-daten sind nicht besonders schützenswert, haben einen geringen Wert	Transaktionsdaten haben mittleren Wert, brauchen jedoch nicht explizit gegen Manipulation gesichert werden	Transaktionsdaten haben hohen Wert und sind besonders schützenswert (z. B. gegen Betrug), nachweisliche Integrität ist sicherzustellen	Transaktionsdaten haben hohen Wert und sind besonders schützenswert (z. B. gegen Betrug), nachweisliche Integrität kann heute noch nicht sichergestellt werden	4 / 0,72

(Fortsetzung)

Tab. 4.2 (Fortsetzung)

Mehrwertaspekte	Gewichtung	Ausprägung der heutigen Gegenwart - potenzieller Mehrwertbeitrag durch Blockchain & Punkte				Punkte/ gewichtet
		gering			hoch	
		1	2	3	4	
Automatisierung	0,07 / 7 %	Vollauto-matisierte Prozesse und Entscheidungen	Verschiedene digitale Informationsstände, Systeme oder Datenabgleiche (auch Insel-lösungen) erfordern manuelle Prüfungen und Prozessschritte	Manuelle Prozesse- und Entscheidungsschritte, wobei Daten teils bereits in IT-Systemen prozessiert werden	Vollständig manuelle Prozesse- und Ent-scheidungsschritte	2 / 0,14
Vertrauen	0,11 / 11 %	Transaktionen mit sehr geringem/ohne Wert, bei dem Vertrauen nicht entscheidend ist	Transaktionen mit kleinem Wert, wobei Partner bekannt sind, denen Vertrauen entgegen-gebracht wird	Transaktionen mit höherem Wert, die auch bei bekannten Partnern zu prüfen sind	Interaktion mit fremden Partnern, denen nicht vertraut wird und Transaktionen zwangsläufig zu veri-fizieren sind	3 / 0,33
Audit	0,1 / 10 %	Audits oder Eingriffe durch Regulierungs-behörden finden nicht statt	Audits sind weitestgehend standardisiert und Daten dement-sprechend auf-bereitet	Teilstandardisierte Audits wofür Daten zur Prüfung weitestgehend zentral zur Verfügung stehen	Keine Standardisierung der Audits, Daten sind nicht aufbereitet und auch nicht zentral ver-fügbar	3 / 0,3

(Fortsetzung)

Tab. 4.2 (Fortsetzung)

Mehrwertaspekte	Gewichtung	Ausprägung der heutigen Gegenwart - potenzieller Mehrwertbeitrag durch Blockchain & Punkte				Punkte/ gewichtet
		gering			hoch	
		1	2	3	4	
Datenqualität	0,05 / 5 %	Digitale, automatisch erzeugte Daten mit hoher Datenqualität	Medien- und Systembrüche führen zu Fehlern in den Daten, jedoch ohne erhebliche Konsequenzen	Medien- und Systembrüche führen zu Fehlern in den Daten, die Prozesse und Entscheidungen negativ beeinflussen	Ausschließlich analoge Erzeugung und Verteilung der Daten, die Auswertungen nur manuell ermöglichen	2 / 0,1
Datennutzung	0,05 / 5 %	Im Prozess werden kaum Daten erzeugt, die gewinnbringend für Analysen eingesetzt werden könnten	Digitale, aggregierte Daten liegen vor und werden gewinnbringend eingesetzt (Analyse als Basis für neue Services, Effizienzsteigerungen, etc.)	Insellösungen verhindern ganzheitliche Sicht auf den Sachverhalt, wodurch bekannte, gewinnbringende Analysepotenziale kaum genutzt werden können	Analoge Daten verhindern die Nutzung ggf. bekannter Analysepotenziale	3 / 0,15
Summe						**3,21**

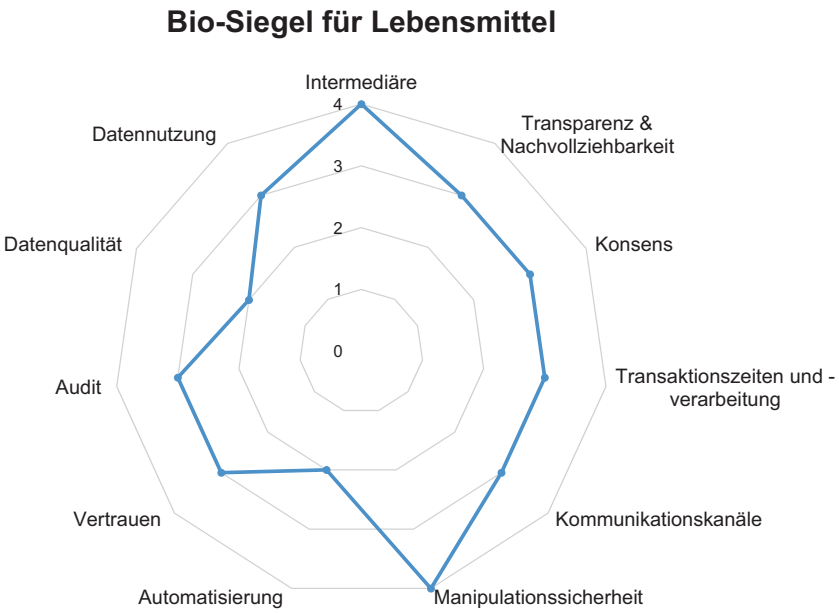

Abb. 4.7 Auswertung: Mehrwerte durch Blockchain für den Anwendungsfall „Bio-Siegel" auf Basis des Mehrwert-Indikationsmodells. (Eigene Darstellung)

Literatur

1. Wirtschaftslexikon. (2015). *Mehrwert*. Abgerufen am 24.08.2019 von Wirtschaftslexikon: http://www.wirtschaftslexikon.co/d/mehrwert/mehrwert.htm
2. Sautet, F. (2014). Schumpeterian Rents. In M. Augier, & D. Teece, *The Palgrave Encyclopedia of Strategic Management* (S. 1–3). London: Palgrave Macmillan.
3. Schumpeter, J. (1939). *Busines Cycles – A Theoretical, Historical and Statistical Analysis of the Capitalist Process.* New York: McGraw-Hill.
4. Coase, R. (1937). *The Nature of the Firm. Economica*, 4(16), 386-405.
5. Ketokivi, M./Mahoney, J. (2017). *Transaction Cost Economics as a Theory of the Firm, Management, and Governance.* o. O.: Oxford Research Encyclopedia of Business and Management.
6. Mecke, I. (19. Februar 2018). *Transaction Cost Economies*. Abgerufen am 15. Juli 2018 von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/transaction-cost-economies-50806/version-274022
7. Williamson, O. (Oktober 1979). Transaction-Cost Economics: The Governance of Contractual Relations. *Journal of Law and Economics, 22*(2), 233–261.

8. Zott, C./Raphael, A./Lorenzo, M. (2011). The Business Model: Recent Developments and Future Research. *Journal of Management, 37*(4), 1019–1042.
9. Pfeifer, A. (2003). *Zum Wertbeitrag von Informationstechnologie – Eine Darstellung an Unternehmen der Fertigungsbranchen in Deutschland.* Passau: o. V.
10. Karimi, J./Somers, T./Gupta, Y. (2001). Impact of Information Technology Management Practices on Customer Service. *Journal of Management Information Systems, 17*(4), 125–158.
11. Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework. *Bus Inf Syst Eng, 59*(6), 385–409. doi:https://doi.org/10.1007/s12599-017-0506-0
12. Schwarz, M. (31. Okotober 2017). *Blockchain-Technologie – Hype oder digitaler Mehrwert?* Abgerufen am 16.11.2019 von KMA-Online: https://www.kma-online.de/aktuelles/it-digital-health/detail/hype-oder-digitaler-mehrwert-a-36036
13. Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain.* o. O.: o. V.
14. O'donnell, T./Plansky, J./Richards, K. (2016). A Strategist's Guide to Blockchain. *strategy + business magazine*(82).
15. Andersen, N. (2016). *Vorstellung der Blockchain-Technologie.* Berlin: Deloitte.
16. Gantner, T./Nack, D./Schwarz, M./Schwarz, R./Winkler, J. (2017). *Blockchain: Die Demokratisierung des Gesundheitswesens?* Leipzig: Wissenschaftliches Institut für Gesundheitsökonomie und Gesundheitssystemforschung.
17. Gupta, M. (2017). *Blockchain for dummies.* Hoboken: John Wiley & Sons, Inc.
18. Rückeshäuser, N. (2017). Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls. (J. Leimeister, & W. Brenner, Hrsg.) *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik*, 16–30.
19. Burghardt, T./Krause, E./Nack, D./Schmidt, M./Treder, T.-M./Velamuri, V. (2016). *Blockchain Technology and the Financial Services Market – State-of-the-Art Analysis*. Leipzig: Infosys Consulting.
20. Taylor, S. (2015). *Blockchain: understanding the potential.* o. O.: Barclays.
21. Swan, M. (2015). *Blockchain – Blueprint For A New Economy.* Sebastopol: O'Reilly Media.
22. Czarnecki, C., Schneider, D., & Wisselink, F. (2017). *Qualitative Wertschöpfungsanalyse von Anwendungsfällen des Narrowband Internet of Things*. In T. Barton, F. Herrmann, V. Meister, C. Müller, & C. Seel, Angewandte Forschung in der Wirtschaftsinformatik – Prozesse, Technologie, Anwendungen, Systeme und Management (S. 184–193). Brandenburg a.d. Havel: mana-Buch.
23. BMG (9. September 2019). Das E-Rezept kommt. Abgerufen am 25.11.2019 von BMG: https://www.bundesgesundheitsministerium.de/e-rezept.html
24. AMG, Arzneimittelgesetz – *Gesetz über den Verkehr mit Arzneimitteln* – § 48 Verschreibungspflicht.
25. Statista. (2019a). *Gesamtzahl öffentlicher Apotheken in Deutschland in den Jahren 1999 bis 2018*. Abgerufen am 25.11.2019 von Statista: https://de.statista.com/statistik/daten/studie/5063/umfrage/oeffentliche-apotheken-in-deutschland-seit-1999
26. Statista. (2017). *Anzahl der Arztpraxen in Deutschland nach Facharztbezeichnung in den Jahren 2007 bis 2015.* Abgerufen am 25.11.2019 von Statista: https://de.statista.com/statistik/daten/studie/281526/umfrage/anzahl-der-arztpraxen-in-deutschland-nach-facharztbezeichnung/

27. GKV Spitzenverband (01. Januar 2020). Die gesetzlichen Krankenkassen. Abgerufen am 13.01.2020 von GKV Spitzenverband: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp
28. Dowideit, A. (08. Mai 2016). *Millionenbetrug in Apotheken mit „Luftrezepten“*. Abgerufen am 23.10.2019 von Welt – Wirtschaft: https://www.welt.de/wirtschaft/article155132175/Millionenbetrug-in-Apotheken-mit-Luftrezepten.html
29. Krankenkassen Deutschland (2020). *Zuzahlungen und Befreiung von der Zuzahlung*. Abgerufen am 13.01.2020 von Krankenkassen Deutschland: https://www.krankenkassen.de/gesetzliche-krankenkassen/leistungen-gesetzliche-krankenkassen/gesetzlich-vorgeschriebene-leistungen/zuzahlungen/
30. Statista. (2019b). *Umsatz mit Bio-Lebensmitteln in Deutschland in den Jahren 2000 bis 2019*. Abgerufen am 25.11.2019 von Statista: https://de.statista.com/statistik/daten/studie/4109/umfrage/bio-lebensmittel-umsatz-zeitreihe/
31. Statista. (2019c). *Anzahl der Produkte mit Bio-Siegel in Deutschland in den Jahren 2004 bis 2019*. Abgerufen am 25.11.2019 von Statista: https://de.statista.com/statistik/daten/studie/421382/umfrage/produkte-mit-bio-siegel-in-deutschland/
32. Lies, J. (14.02.2018). Harte und weiche Faktoren. Abgerufen am 06.09.2019 von Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/harte-und-weiche-faktoren-52688/version-275806
33. Wübbenhorst, K./Eggert, W./Minter, S./Gillenkirch, R. (19.02.2018). *Nutzwertanalyse*. Abgerufen am 13.09.2019 von Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/nutzwertanalyse-42926/version-266266
34. Yoo, C. (2015). *Moore's Law, Metcalfe's Law, and the Theory of Optimal Interoperability.* o. O.: Faculty Scholarship.

Auswirkung der Blockchain auf Geschäftsmodelle und Ökosysteme

5

Auf Grundlage der Architektur und Funktionsweise der Blockchain stellt diese Technologie viele bestehende Konzepte infrage. Begriffe wie Geld, Eigentum, Regierung oder Souveränität können mittels Blockchain auf innovative Weise neu definiert werden [1]. In vielen Bereichen wird Blockchain als neue, digitale Form der Demokratie bezeichnet, da Entscheidungen basisdemokratisch erfolgen. Alle Peers (bzw. eine definierte Menge für den Konsens) im Netzwerk stimmen einer Transaktion vor ihrer Ausführung zu. Gleichzeitig wird Blockchain oftmals als Cutting Edge Technologie gesehen, die nahezu jede Branche verändern kann. In diesem Kapitel werden mögliche Auswirkungen der Blockchain-Technologie auf bestehende Geschäftsmodelle sowie Ökosysteme zusammenfassend betrachtet sowie potenzielle Entwicklungen aufgezeigt.

Aus heutiger Perspektive lässt sich der technologische Einfluss der Blockchain in drei Stufen untergliedern, wobei die Stufen unterschiedlich definiert werden. Höltmann und Vasilev untergliedern 1) operative Exzellenz (Abschn. 5.1), 2) inkrementelle Optimierung (Abschn. 5.2) sowie 3) neue Geschäftsmodelle und Ökosysteme (Abschn. 5.3) [2]. Diese Aufgliederung ermöglicht zudem die Einordnung des eigenen Unternehmens und Geschäftsmodells in die Chancen und Möglichkeiten der Distributed Ledger Technologie. Weiterhin erläutern Beispiele, wie eine Positionierung innerhalb dieser Ökosysteme erfolgen kann und wie sich zukünftig Mehrwertdienste realisieren lassen. Das Prüfen von Daten sowie die Position als Mittelsmann innerhalb etablierter Ökosysteme wird voraussichtlich in Zukunft kein elementarer Bestandteil der Wirtschaft mehr sein.

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_5

5.1 Operative Exzellenz

Als operative Exzellenz (1) definieren Höltmann und Vasilev den Einsatz der Blockchain zur Automatisierung von (grenzüberschreitenden) Prozessen bzw. Transaktionen und gleichzeitiger Prüfung bestehender Regularien durch Smart Contracts. Ergebnis sind Kostenersparnisse, signifikant schnellere Prozesse sowie effizientere Sicherheits-, Compliance- und Reporting-Mechanismen [2]. Melanie Swan, die sich mit Blockchain als Basis für eine neue Ökonomie beschäftigt, bezeichnet diese erste Stufe als Blockchain 1.0. Sie beschreibt zunächst ein digitales Zahlungssystem *(Internet of Money).* Neben digitalem Bargeld bietet Blockchain im Kern zugleich ein offenes, programmierbares Netzwerk für den dezentralen Handel aller Ressourcen [1].

Anwendungsfall: eRezept Der Anwendungsfall zum eRezept (Abschn. 4.3.2.1) lässt sich dieser ersten Entwicklungsstufe der Blockchain zuordnen. Smart Contracts, mit Anbindung an weitere Systeme über Orakel, automatisieren Prozessabläufe. Definierte Transaktionsregeln werden gleichzeitig bei jeder Transaktion geprüft sowie bei Bedarf entsprechende Folgeprozesse angestoßen. Intermediäre oder zentrale Netzwerkkomponenten sind in der Kommunikation nicht erforderlich, da Transaktionen direkt Peer-2-Peer zwischen den teilnehmenden Parteien erfolgen. In Summe kann der Prozessablauf effizienter und kundenfreundlicher gestaltet werden.

Anwendungsfall: Umweltbedingungen innerhalb von Lieferketten Ein weiteres Beispiel für die operative Exzellenz ist die Abbildung von Lieferketten (auch als Supply Chain bezeichnet) in einem Blockchain-Netzwerk, indem Prozessschritte automatisiert transparent getrackt und bestehende Regularien gleichzeitig fortlaufend überprüft werden.

Lieferketten sind durch die Globalisierung der Handelsnetzwerke sowie aufgrund immer komplexerer Produkte deutlich umfangreicher und undurchsichtiger geworden. Im Ergebnis befinden sich viele einzelne Akteure innerhalb einer Supply Chain, die zudem oft über mehrere Länder und Kontinente verteilt sind. Die Transportwege über Land, Wasser und Luft sind vielseitig und meist schwer im Einzelnen nachzuvollziehen. Insbesondere für Lebensmittel, Medikamente oder Spezialprodukte sind Umweltbedingungen wie Temperatur oder Luftfeuchtigkeit während des Transports entscheidend, um eine einwandfreie Qualität sicherzustellen. Gegenwärtig lässt sich eine konstante Kühlkette nur schwer belegen, da die Vielzahl unterschiedlicher Parteien und Systeme keine Transparenz und vertrauenswürdige Nachvollziehbarkeit der Produktzustände abbilden

kann. Für den letzten Akteur einer Lieferkette ist es weiterhin zumeist nicht möglich, den Ursprung der einzelnen Produktbestandteile zu verorten.

Mittels im Fachtraum oder Schiffscontainer angebrachter Sensoren lassen sich die Umweltbedingungen, denen ein Produkt ausgesetzt ist, permanent aufzeichnen. In Kombination mit dem Internet der Dinge (Internet of Things, kurz IoT) können diese Daten geteilt und analysiert werden (z. B. Überschreitungen vorgegebener Parameter werden automatisch gemeldet). Um die gesamte Lieferkette transparent zu gestalten sowie das Vertrauen bis ins letzte Kettenglied zu garantieren, gilt es, diese Daten durchgängig zu Teilen und gleichzeitig die Unveränderlichkeit sicherzustellen. Das Vertrauen, welches geprüfte und zertifizierte Sensoren für die Datenerhebung darstellen, stellt Blockchain für die Datenübertragung und Datenspeicherung dar. Befinden sich alle Akteure einer Lieferkette innerhalb eines Blockchain-Netzwerkes, können deren Sensorboxen etwaige Überschreitungen vorgegebener Parameter in der Blockchain teilen. Auf Basis dieser Daten lassen sich automatisch weitere Folgeaktionen mit Hilfe von Smart Contracts anstoßen. Alternativ kann die Aufgabe der Datenspeicherung und Verarbeitung durch eine zentrale, vertrauenswürdige Stelle (wie bspw. Regierungsorganisation, Unternehmen für Qualitätssicherung, Transportdienstleister) innerhalb des Ökosystems abgebildet werden. Es ist jedoch eher unwahrscheinlich, dass sich alle Teilnehmer der globalen Supply Chain auf eine Organisation einigen, zudem sich die einzelnen Akteure somit abhängig von einem Intermediär machen, der zudem zusätzliche Prozess- und Administrationskosten verursacht.

Zusätzlich kann die Blockchain-Technologie die Effizienz innerhalb der Lieferkette, insbesondere bzgl. der Administration und Zahlung, steigern. Mit Smart Contracts lassen sich automatisch alle notwendigen Informationen sowie Zahlungen (wie Reklamationen oder Transportgebühren) zwischen den einzelnen Parteien abwickeln. Darüber hinaus lassen sich komplexe Produkte besser bzw. überhaupt erst recyceln, wenn die einzelnen Komponenten zu ihrem Ursprung zurückverfolgt werden können und somit wichtige Informationen über die Materialzusammensetzung bekannt sind (gilt insb. für Kunststoffe).

Zusammenfassung Im Kern lässt sich der Aspekt der operativen Exzellenz als Effizienzsteigerung innerhalb bestehender Ökosysteme und Geschäftsprozesse zusammenfassen. Der Fokus liegt auf der Reduzierung der Schnittstellen, indem Blockchain einen *Single Point of Entry* darstellt. Befindet sich eine Organisation in dem Blockchain-Netzwerk, kann diese sofort mit allen anderen Organisationen Transaktionen austauschen. Individuelle Schnittstellen (z. B. Anbindung zweier Systeme, telefonischer Austausch, Versand von Papierunterlagen) entfallen und führen zu Kostenersparnissen. Gleichzeitig wird die Datenqualität durch Reduzierung der System- und Medienbrüche erhöht.

Weiterhin beschreibt die operative Exzellenz die zunehmende Automatisierung der Prozesse. Da jede Transaktion innerhalb der Blockchain vor Durchführung gegen die definierten Transaktionsregeln (in den Smart Contracts abgebildet) geprüft und anschließend unveränderbar im Netzwerk gespeichert wird, kann die Datenbasis in der Blockchain als vertrauensvoll *(Single Point of Truth)* bezeichnet werden. Auf dieser Grundlage lassen sich Vorgänge automatisiert abbilden, die bisher durch Menschen manuell durchzuführen oder zu bestätigen waren, um Fehler zu vermeiden und Vertrauen zu schaffen.

5.2 Inkrementelle Optimierung

Die inkrementelle Optimierung (2) beschreibt dahingegen den stufenweisen Fortschritt bzw. Weiterentwicklung bestehender Geschäftsmodelle. Durch u. a. weitere Prozessoptimierungen und transparentere Angebotsprozesse, können ergänzende bzw. neue Dienstleistungen oder Produkte angeboten werden [2]. Swan, die den Begriff Blockchain 2.0 verwendet, beschreibt diese Stufe, als die Dezentralisierung von Märkten, wobei sich alle Arten von Vermögenswerten, Verträgen oder sonstigen Wirtschaftsgütern in einer Blockchain abbilden und übertragen lassen [1].

Anwendungsfall: Mikroversicherungen Ein Beispiel für einen neuen Servicebereich stellen Mikroversicherungen dar. Mikroversicherungen sind Kleinstversicherungen, die vielfältige, meist elementare Risiken, angepasst an die individuellen Lebenssituationen der Kunden, absichern. Diese Versicherungen decken, oftmals bei geringen Beitragssätzen, konkret ein Ereignis, z. B. Krankheit oder Unfall ab. Gegenwärtig dienen die Versicherungen vorwiegend zur Grundsicherung in Entwicklungsländern [3]. Insbesondere der Fortschritt mobiler sowie digitaler Infrastrukturen fördern das Wachstum der Mikroversicherungen. Mobile Endgeräte bilden den vorrangigen Kommunikationskanal und reduzieren die Verwaltungskosten innerhalb der Versicherungsgesellschaften aufgrund der Digitalisierung und Automatisierung erheblich. Die mobile Mikrokrankenversicherung bimaAFYA konnte ihre Verwaltungskosten in Tansania auf Basis der Blockchain-Technologie erstmals um 99 % senken. Alle Versicherungsvorgänge wie der Vertragsabschluss, die Prämienzahlung, das Leistungsmanagement und die Krankenhausansprüche werden vollends digital abgebildet [4].

In den Industriestaaten finden Mikroversicherungen bisher weniger Anwendung, da günstige Versicherungstarife oftmals aufgrund der hohen Prozesskosten (Administrations- und Transaktionskosten) aufseiten der Versicherung nicht lukrativ sind. Bei niedrigpreisigen Versicherungen zum Schutz von Konsumgütern, wie bspw. Handys, Fahrrädern oder Musikinstrumenten,

bietet Blockchain jedoch eine potenzielle Funktion [4]. In der Blockchain könnte der Versicherungsvertrag direkt zwischen der versicherten Person, dem Versicherungsgeber und ggf. dem Verkäufer des Produktes geschlossen werden. Die Zahlung erfolgt innerhalb der Blockchain bspw. mittels einer Kryptowährung. Erst bei eingetretenem Schadensfall werden Prozesse in der Versicherung angestoßen. Wird ein Schadensfall gemeldet, prüft das Versicherungsunternehmen in der Blockchain den Vertrag, erfolgte Prämienzahlungen sowie ggf. zusätzliche Parameter (bspw. Statusangaben von, zur Sicherung verwendeter, IoT-Geräte). Der Vorteil der Blockchain besteht in der transparenten Nachvollziehbarkeit sowie der manipulationssicheren Datenspeicherung. Keiner der Parteien ist es möglich, registrierte Daten im Nachgang zu verändern, um Zahlungen zu seinen Gunsten herbeizuführen bzw. abzuwenden [5].

Ein weiteres Beispiel für Mikroversicherungen in vorwiegend Industriestaaten sind Flugversicherungen, die im Fall von Flugverspätungen oder Ausfällen Schadensersatzleitungen an die Kunden auszahlen. Wie oben bereits beschrieben, werden die Versicherungsverträge sowie Beitragszahlungen über die Blockchain abgewickelt. Smart Contracts prüfen bei Abschluss der Versicherung, ob der Kunde das Ticket tatsächlich gekauft hat. Orakel ermöglichen den Abgleich der Buchungsdaten mit der Fluggesellschaft. Möglich ist diese Art der Kleinversicherung jedoch erst dann, wenn auch die Prüfung des Schadensfalls und Auszahlung der Entschädigung automatisiert erfolgt. Das Anbinden einer Flugverspätungsdatenbank (über Orakel) kann die für die Schadensfeststellung erforderlichen Daten liefern. Wird nur eine Datenbank eingebunden, besteht jedoch das Risiko eines *Single Point of Failure.* Ein Angreifer braucht nur eine Datenbank anzugreifen bzw. zu manipulieren um eine Auszahlung auszulösen. Sowohl die Robustheit als auch die Manipulationssicherheit, zwei der Blockchain-Kerneigenschaften, wären eingeschränkt. Um dies zu umgehen, lassen sich mehrere, voneinander unabhängige Flugverspätungsservices und Datenbanken einbinden. Nur wenn der Konsens dieser Daten eine Entschädigung begründen, wird eine Auszahlung herbeigeführt. Diese Art der Datenquellen wird auch als *distributed Datasource,* zu Deutsch verteilte Datenquellen, bezeichnet. Voraussetzung für einen erfolgreichen Angriff wäre es, dass der potenzielle Angreifer alle Datenquellen zum gleichen Zeitpunkt in genau gleicher Weise manipuliert. Ein vergleichbares Versicherungsprinzip wurde von der Axa 2017 [6] erstmals vorgestellt und pilotiert.

Anwendungsfall: Bio-Siegel für Lebensmittel Ebenfalls unter dem Aspekt der inkrementellen Optimierung bzw. Weiterentwicklung des bestehenden Geschäftsmodells lässt sich der Anwendungsfall der Blockchain-basierten Bio-Siegel betrachten (Abschn. 4.3.2.2). Die Kernidee, Bio-Lebensmittel nach erfolgreicher

Zertifizierung der z. B. Betriebe entsprechend zu kennzeichnen, ist weiterhin unverändert. Um die Lösung jedoch nachhaltig abzusichern und auf einer stabilen Basis weiterentwickeln zu können, fehlt derzeit das Vertrauen im Netzwerk. Für weiterverarbeitende Betriebe innerhalb der Lieferkette oder den Endverbraucher gibt es keine sichere Möglichkeit, die Echtheit der Siegel oder die Verknüpfung zwischen dem Siegel und dem Produkt zu prüfen. Wie in Kap. 2 beschrieben, kann Blockchain diese Lücke schließen und bildet eine Erweiterung des bestehenden Geschäftsmodells um den zusätzlichen Service der sicheren Verifikation der Siegel und Produkte. Weiterhin bilden das neue Vertrauen sowie die Transparenz zusätzliche Mehrwerte für das Ökosystem.

Zusammenfassung In Summe kann das Prinzip der inkrementellen Optimierung in beiden Beispielen für die beteiligten Unternehmen einen neuen, zusätzlichen Geschäftszweig bilden, der zusätzliche Einnahmen mit geringem Aufwand generiert. Vorrangig dient Blockchain hierbei als Komponente, die Vertrauen und Transparenz in das Netzwerk einbringt. Im Vergleich zur Blockchain 1.0 geht es nicht mehr primär bzw. ausschließlich um die Automatisierung und das Schaffen einer gemeinsamen Datenbasis. Gegenüber der Blockchain 3.0 (neue Geschäftsmodelle und Ökosysteme) dienen die hier noch im Netzwerk beteiligten Unternehmen primär als Sicherungskomponente. Das Versicherungsunternehmen im Anwendungsfall für die Flugversicherung deckt etwaige Kapitalrisiken ab (z. B. im Fall von Großschadenslagen), insbesondere für den Fall, dass die Entschädigungssumme das im Netzwerk eingezahlte Kapital übersteigen. Im Fall der Bio-Siegel dient die Biosiegel-Kontrollstelle der Prüfung der Betriebe und der Erstellung der Siegel im Netzwerk. Initial ist dieser Stelle jedoch zu vertrauen, dass vorgegebene Richtlinien bei der Prüfung eingehalten werden. Die Besetzung dieser Position durch eine Regierungsstelle sowie das Teilen von Laborproben der Lebensmittel innerhalb der Blockchain können das Vertrauen stützen.

Als klassische Intermediäre, die die Kommunikation und Abläufe im Netzwerk bündeln, sind diese Teilnehmer jedoch nicht zu verstehen. Vielmehr können auch mehrere Versicherungen oder Biosiegel-Kontrollstellen gleichzeitig Teil des Netzwerkes werden.

5.3 Neue Geschäftsmodelle und Ökosysteme

Weiterführend kann Blockchain neue Geschäftsmodelle sowie Ökosysteme (3) schaffen. Dabei wird der Begriff Smart Contract auf Smart Legal Contracts ausgeweitet, indem Geschäftspartner ihre Verträge einzig basierend auf digitalen

Protokollen abschließen. Vertragsklauseln sowie Besitzverhältnisse werden elektronisch identifiziert und transparent nachvollziehbar [2]. Neben realen Personen, wird der Begriff Geschäftspartner im Sinne der Blockchain 3.0 auf Dapps, DAOs, DACs oder DASs (Distributed Applications, Distributed Autonomous Organizations, Distributed Autonomous Corporations oder Distributed Autonomous Societies) ausgeweitet. In diesem Sinne beschreibt die dritte Stufe zudem eine mögliche Weiterentwicklung, in der komplexe Smart (Legal) Contracts als autarkes Unternehmen agieren können [1]. Abb. 5.1 beschreibt den schematischen Aufbau einer DAO und die Einordnung in das Netzwerk. Essenziell ist die Autonomie der DAO, die eigenständig Transaktionen mit Vertragspartnern durchführt, welche durch die *Eigner* des Netzwerkes mittels Votingsystem jedoch beeinflusst werden könnten.

Zusätzlich dient Blockchain in diesem Zusammenhang als *Enabler* Technologie. Mit Hilfe von künstlicher Intelligenz werden Entscheidungen automatisiert und neue Erkenntnisse aus Daten gewonnen. Das Internet der Dinge verknüpft Maschinen untereinander, automatisiert deren Interaktionen und kann Gegenstände mithilfe der KI bis zu einem gewissen Grad *intelligent* machen. Auf dieser Basis lassen sich Vorgänge zunehmend automatisieren sowie neue Dienstleitungen anbieten. In der Umsetzung spielen Daten eine zentrale Rolle

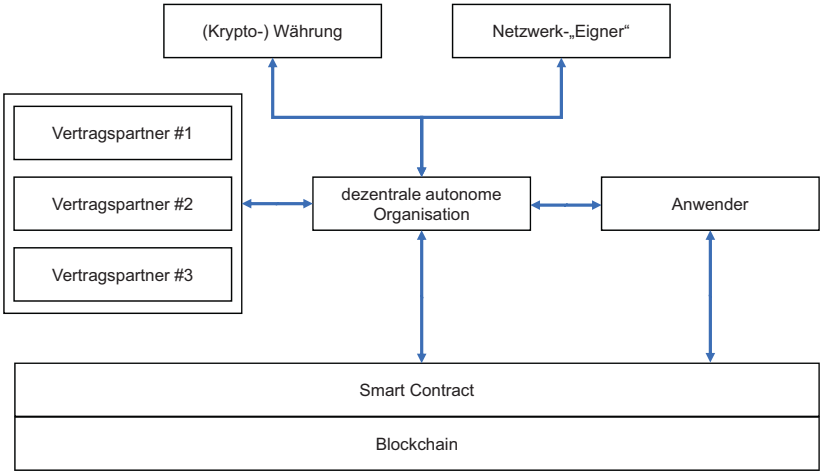

Abb. 5.1 Schematischer Aufbau einer dezentralen autonomen Organisation. (Eigene Darstellung in Anlehnung an Verhoelen 2017, S. 5)

und die Qualität der Daten ist ausschlaggebend für die Qualität des Ergebnisses bzw. der Dienstleistung. Hier entfaltet sich der Kernmehrwert der Blockchain-Technologie. Eine im Netzwerk einheitliche, vertrauenswürdige und nicht manipulierbare Datenbasis, die zugleich mit Hilfe der Smart Contracts qualitätsgesichert ist, bildet demnach das Fundament für die Entwicklung vollständig neuer Geschäftsmodelle und Ökosysteme. Manuelle Datenprüfungen und Datensilos innerhalb von Organisationen entfallen demnach in Gänze.

Anwendungsfall: Peer-2-Peer Versicherungen Ein Beispiel für ein neues Geschäftsmodell bilden auf Blockchain basierende Peer-2-Peer Versicherungen, die weitestgehend ohne eine zentrale Versicherungsgesellschaft auskommen. Teambrella erprobt diese neue Versicherungsform seit 2017 in zunächst vier Pilotprojekten verschiedener Versicherungssparten [7]. Die Netzwerkteilnehmer, die sich gegenseitig Peer-2-Peer versichern, behalten die Kontrolle über ihre Versicherung und nehmen die Risikobewertung sowie Entscheidung über eine Auszahlung eigens vor. Anstelle der Versicherungsgesellschaft, verwalten sich Teams, bestehend aus mehreren Netzwerk-Peers, selbst. Alle Entscheidungen werden innerhalb des Teams getroffen. Zur Abstimmung wird ein Voting-Verfahren eingesetzt, wobei sich das Stimmgewicht jedes Teilnehmers nach der individuellen Prämienzahlung richtet. Schäden werden durch den betroffenen Teilnehmer direkt in der Blockchain gemeldet. Bilder oder Dokumente können zusätzlich über Teambrella geteilt werden, auch wenn sich diese nicht durch die Blockchain-Technologie verifizieren lassen. Das Team stimmt, anhand im Vorfeld definierter Regeln, über die Höhe der Entschädigung ab. Die Höhe der Regulierung errechnet sich aus dem Mittelwert der einzelnen Stimmen, wobei die Erstattung zwischen 0 und 100 % des Schadens betragen kann [8].

Um diese Art der Versicherungen künftig auszubauen, wird ein Mechanismus, der einen gemeldeten Schaden verifiziert, zwingend erforderlich. Am Beispiel einer Versicherung für Smartphones wäre die Einbindung von Handyreparaturdiensten denkbar. Diese verifizieren den Schaden in der Blockchain, wobei sie selbst mittels *sozialer Ächtung* (bspw. mittels Up & Down Rating) bewertet werden. Ziel ist es, eine ehrliche, realistische und faire Validierung zu erzielen.

Anwendungsfall: mobilityDAO Die unter Blockchain 3.0 aufgeführten neuen Ökosysteme bilden automatisierte bzw. autonome Märkte. Transaktionen werden auf Basis sich dynamisch entwickelnder Bedingungen und definierten Regularien (Vorgaben, zur Gültigkeit von Transaktionen) autark durchgeführt [1]. Autonome

Mobilitätsdienstleister, bzw. selbstfahrende Autos in Eigenbesitz, bilden ein Beispiel für diese Art der auf Blockchain basierenden Märkte. Statt einer zentralen Plattform wie z. B. Uber, könnte zukünftig eine mobilityDAO die *Robo-Taxis* organisieren. Sind die Regeln für die teilnehmenden Fahrzeuge zu Beginn einmal definiert und als Smart Contract in der Blockchain etabliert, ist die mobilityDAO als sich selbst verwaltender Algorithmus anzusehen. Im Vorfeld sind bspw. der Umgang mit Reservierungen, die allgemeinen Beförderungsbedingungen sowie der Handel mit Service-Anbietern, wie Tankstellen, Waschstraßen, Werkstätten oder Mautstellen, zu definieren. Die Blockchain garantiert für das Vertrauen zwischen den Teilnehmern und bietet die notwendige Sicherheit im allgemeinen Wirtschaftsverkehr. Alle Vorgänge, wie Verträge, Reservierungen oder Zahlungen können direkt Peer-2-Peer über die Blockchain abgewickelt sowie sicher gespeichert werden, ohne weitere, externe Instanzen einzubinden. Für den Zahlungsverkehr ist ein mobility-Token denkbar, wodurch das System zusätzlich grenzübergreifend agieren kann. Die menschlichen Nutzer sowie die Fahrzeuge bilden die Netzwerkknoten [9]. Für den Netzwerkzugriff benötigen die Endnutzer entweder einen eigenen Netzwerkknoten, der sich perspektivisch als kleines Hardware-Gerät abbilden lässt oder aber eine Organisation, die die Verwaltung der Netzwerkknoten und Krypto-Wallets ermöglicht. Krypto-Wallets sind zweckmäßig vergleichbar mit heutigen Bankkonten, in denen Netzwerknutzer ihre Token speichern können. Ggf. ist die Verwaltung, Sicherung und zur Verfügungstellung der Wallets ein mögliches neues Geschäftsmodell für heutige Banken oder IT-Provider.

Zusammenfassung Insbesondere Transaktionen mit den Servicediensten stellen vorwiegend Maschine-zu-Maschine-Kommunikationen dar. Blockchain verknüpft die Interaktion von Maschinen (IoT) mit einem Ansatz künstlicher Intelligenz, der Einzug in die Smart Contracts erhalten kann. Der KI-Einsatz ermöglicht dem Netzwerk ein schnelles und flexibles Reagieren auf sich ändernde Umwelteinflüsse bzw. Anforderungen [1]. Im Kern ist Blockchain als Basisnetzwerkkomponente anzusehen, die vertrauensvolle Transaktionen zwischen Maschinen und Menschen, als auch zwischen Maschinen untereinander ermöglicht. Weiterhin bildet die Blockchain eine vertrauensvolle Datenbasis ab und garantiert die Prüfung aller Transaktionen gegenüber der vereinbarten Geschäftslogik. Die Fahrzeuge handeln innerhalb der zu Beginn vordefinierten Rahmenbedingungen teilautonom. Transaktionskosten werden durch den Wegfall der Serviceanbieter wie z. B. Uber minimiert [9].

Literatur

1. Swan, M. (2015). *Blockchain – Blueprint For A New Economy.* Sebastopol: O'Reilly Media.
2. Höltmann, A./Vasilev, O. (2016). *Wenn der Blockchain-Nebel sich lichtet – Vom Hype zum Geschäftsmodell.* o. O.: Accenture.
3. BZE. (2020). Mikroversicherungen. Abgerufen am 20.01.2020 von Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung: https://www.bmz.de/de/themen/soziale_sicherung/deutsches_engagement/mikroversicherungen/index.html
4. Mehta, D./Berthelmann, T. (2017). *InsurTech – Statista Report 2017.* Hamburg: Statista.
5. Morabito, V. (2017). *Business Innovation Through Blockchain.* Mailand: Springer.
6. Klostermeier, J. (18. Januar 2018). *Axa startet erste Blockchain-Versicherung*. Abgerufen am 23.10.2019 von CIO: https://www.cio.de/a/axa-startet-erste-blockchain-versicherung,3563749
7. Teambrella. (2018). *Not insurance. A lot better.* Abgerufen am 02. August 2018 von teambrella: https://teambrella.com/
8. Paperno, A./Kravchuk, V./Porubaev, E. (2017). *Teambrella: A Peer-to-Peer Insurance System.* o. O: O. V.
9. Brandt, J. C./Werner, T. (2018). *Blockchain – Eine Technologie mit disruptivem Charakter.* Düsseldorf: VDI Technologiezentrum GmbH.
10. Verhoelen, J. (29. August 2017). *Decentralized Autonomous Organization – Organisationen auf der Blockchain*. Abgerufen am 01.02.2020 von codecentric – IT-Expertenwissen von Entwicklern für Entwickler: https://blog.codecentric.de/2017/08/decentralized-autonomous-organization-blockchain/

Zusammenfassung

6

6.1 Schlussbetrachtung

Die vertretenden Ansichten zur Zukunft der Blockchain-Technologie sind mindestens genauso kontrovers und divers wie das Wissen Rund um die Funktionsweise, technische Basis, sinnvolle Anwendungsfälle und Mehrwerte dieser Technologie. Auf der einen Seite wird die Ansicht vertreten, dass mit Blockchain eine neue Technologie existiert, die die gesamte Welt fundamental verändern kann. Von der Wirtschaft, dem sozialen Zusammenleben bis zur Art und Weise wie Demokratie heute funktioniert. Auf der anderen Seite existiert die Ansicht, dass Blockchain noch immer ein überhypter Technologie-Trend ist, der in einigen Jahren vollständig an Bedeutung verloren hat, unter anderem aufgrund vieler noch ungeklärter Fragestellungen.

Die wirkliche Entwicklung kann zwar gegenwärtig nicht vorhergesagt werden, dennoch ist davon auszugehen, dass sich die Wahrheit zwischen den beiden kontroversen Meinungen verbirgt. Wie in Kap. 5 dargestellt, lässt sich die Blockchain-Technologie und ihre Implikationen auf heutige Ökosysteme in drei Evolutionsstufen abbilden. Von Blockchain 1.0 als Verbesserung bestehender Prozesse, über die Blockchain 2.0, die bestehende Geschäftsmodelle um neue Angebote ergänzen kann und diese verstärkt optimiert, bis hin zur Blockchain 3.0 als fundamentale Neugestaltung ganzer sozioökologischer Systeme und autonomer Organisationen. Dies zeigt bereits die Bandbreite der grundsätzlichen Möglichkeiten und Auswirkungen dieser Technologie auf, dennoch bestehen aus heutiger Sicht diverse Herausforderungen, die es zuvor zu lösen gilt. Beispielsweise sind klare rechtliche Rahmenbedingungen notwendig, die Vertrags- und Besitzverhältnisse der digitalen Werte in der Blockchain regeln. Rechtssicherheit für das Schließen Blockchain-basierter Verträge oder für den Handel von

N. T. Urban, *Blockchain for Business,*
https://doi.org/10.1007/978-3-658-29822-7_6

Wertpapieren und Krypto-Token ist essentiell. Hier hat der deutschsprachige Raum bereits jetzt eine Vorreiterrolle eingenommen, indem die BaFin und die FINMA drei Arten von Token in Verbindung mit entsprechenden Regularien definiert haben. Diese sind: [1]

- *Payment-Token* (z. B. Bitcoin): diese werden gezielt als privates Zahlungsmittel eingesetzt, während diese Token über keinen weiteren intrinsischen Wert verfügen. Darüber hinaus besteht keine oder nur eine geringe weitere Funktionalität.
- *Security-Token* (Wertpapierähnliche bzw. Equity- und sonstige Investment-Token): Besitzer erhalten mitgliedschaftliche Rechte oder schuldrechtliche Ansprüche vermögenswerten Inhalts, vergleichbar mit heutigen Aktien oder Schuldtiteln.
- *Utility-Token* (Nutzungs- oder Verbrauchstoken): die Nutzung besteht ausschließlich innerhalb des Netzwerkes des Emittenten und dient zum Bezug von Waren oder Dienstleistungen.

Auch hat die Bundesregierung mit der Blockchain-Strategie bekanntgegeben, die regulatorischen Grundlagen zeitnah zu schaffen und dem Markt somit die notwendige Rückendeckung zuzuschreiben [2]. Da die Blockchain-Technologie selbst jedoch nicht an Landesgrenzen gebunden ist, gilt es im nächsten Schritt internationale Vereinbarungen, analog dem internationalen Handelsrecht zu treffen. Hier ist bereits heute festzustellen, dass viele Länder genau beobachten, wie Deutschland bei der Schaffung der regulatorischen Grundlagen vorgeht und wie diese gestaltet werden. Parallel zu den regulatorischen Rahmenbedingungen steht die technologische Umsetzung noch am Beginn der Entwicklung. Besonderes Augenmerk liegt auf der Erhöhung der Transaktionsgeschwindigkeit bei gleichzeitiger Reduzierung der benötigten Ressourcen, im Speziellen die Reduzierung des Energiebedarfs sowie der benötigten Rechenkapazität für den Betrieb des Netzwerkes. Permissioned Blockchain-Implementierungen legen dazu bereits einen wichtigen Grundstein, da hier deutlich effizientere Konsensalgorithmen eingesetzt werden (bei Hyperledger Fabric z. B. Kafka) [3]. Verglichen mit herkömmlichen Datenbanken liegt der Energieverbrauch erfahrungsgemäß nur noch leicht über diesen. Hintergrund ist, dass der äußerst rechenintensive Mining-Prozess, bei dem die Netzwerkteilnehmer (ausschließlich die Miner) um die Wette rechnen, um als erster den neuen Block zu errechnen, entfällt. Prominentes Beispiel für diese Algorithmen ist das Proof-of-Work Verfahren, welches im Bitcoin-Netzwerk eingesetzt ist [4]. Zuletzt gestalten noch fehlende technische Standards die Umsetzung als komplexes Vorhaben. Bspw. sind die unterschiedlichen Blockchain-Frameworks

untereinander nicht kompatibel, weshalb entweder dedizierte Konnektoren (Schnittstellen) zu entwickeln sind oder sich vor Umsetzung eines neuen Anwendungsfalls auf ein Blockchain-Framework zu verständigen ist. In permissionless Implementierungen sind zudem alle Entscheidungen zu Änderungen in den Protokollen bzw. der grundlegenden Architektur durch die Open Community durchzuführen. Zum einen dient dies der Dezentralität und Unabhängigkeit, kann jedoch zu längeren Entscheidungsprozessen führen. Im Fall von permissioned Implementierungen werden derartige Entscheidungen zumeist durch ein Konsortium oder eine bestimmte Gruppe getroffen, die als *Eigner* des Netzwerkes gilt und deren Mitglieder von den Netzwerkteilnehmern gestellt sind.

Doch auf dem Weg zur Umsetzung neuer Blockchain-Projekte gilt es ebenfalls das erforderliche Ökosystem auf Basis des Blockchain-Netzwerkes aufzubauen. Denn die Manipulationssicherheit sowie das Vertrauen in die Transaktionen ist in der Blockchain nur dann gegeben, wenn eine kritische Menge an Netzwerkteilnehmern erreicht ist (vgl. Kap. 2). Weiterhin ergibt sich der Mehrwert dieser Technologie erst durch den Netzwerkgedanken, u. a. indem eine *Single Source of Truth,* eine einheitliche Schnittstelle sowie gemeinsame Geschäftsregeln etabliert werden (vgl. Abschn. 4.2).

Für den Aufbau des Netzwerkes aus typischerweise heutigen Kunden, Lieferanten, Partnern sowie möglicherweise Konkurrenten und Regulatoren, ist es unumgänglich ein klares Verständnis über den Anwendungsfall, die Ziele und Mehrwerte zu haben. Da die verschiedenen Akteure zumeist jedoch unterschiedliche Sichtweisen auf ihre heutige Rolle haben sowie unterschiedliche Zielstellungen verfolgen, ist die Abstimmung sowie Einigung auf eine Ansicht oft schwierig. Doch ist dies der Grundstein für den Aufbau der Blockchain-Anwendung, da ein gemeinsamer Smart Contract die Geschäftslogik beschreibt, basierend auf einem gemeinsamen Daten- und einem gemeinsamen Netzwerk-Governancemodell.

Um das zu erreichen ist die Auswahl, die präzise Untersuchung sowie die klare Definition der potenziellen Anwendungsidee zu Beginn unumgänglich. Diesbezüglich hat das Buch *Kriterien für geeignete Blockchain-Anwendungsfälle* aufgezeigt (Kap. 3). Hierbei ist klar ersichtlich, dass gegenwärtig noch immer viele Blockchain-Projekte scheitern bzw. nicht ausreichend weiterverfolgt werden. Grund ist hierfür u. a. die willentliche Realisierung von Anwendungsfällen, ohne Prüfung, ob Blockchain für die vorliegende Konstellation faktisch die probate Technologie bietet. Demgemäß ist eine explizite Prüfung der Anwendungsidee mittels des dargestellten Entscheidungsmodells (vgl. Abschn. 3.3) sinnvoll. Das Modell kann zudem als Fundament für Workshops dienen und insbesondere im Internet publizierte Mainstream-Ideen von konkreten Anwendungsfällen differenzieren.

Analog gilt dies gleichfalls für die *Untersuchung der Mehrwerte,* die das Fundament für die organisatorische Skalierung des Netzwerkes bildet (Kap. 4). Im Buch ist aufgezeigt, dass sich die in der Fachliteratur publizierten Mehrwerte weitestgehend kongruent untereinander verhalten (vgl. Abschn. 4.2). Auch hat sich gezeigt, dass Mehrwerte bisher primär allgemein beschrieben sind, es gegenwärtig jedoch keine direkten, strukturierten Ansätze gibt, Mehrwerte von Blockchain im Kontext eines konkreten Anwendungsfalls zu betrachten (Abschn. 4.3). Dieses Defizit füllt das Indikationsmodell als Resultat der zweiten zentralen Fragestellung (Abschn. 4.4). Das Ergebnis dieses Modells kann in Verbindung mit dem Spinnendiagramm zugleich als Motivationsbasis für potenzielle Teilnehmer dienen, sich dem Blockchain-Netzwerk anzuschließen (Klarstellung des Mehrwertes).

In Summe spiegeln sich die wesentlichen Ergebnisse dieses Buches insbesondere in den drei zentralen Fragestellungen wider (vgl. Abschn. 1.2):

1. Welche Kriterien sollten für einen erfolgreichen Blockchain-Anwendungsfall berücksichtigt werden?
2. Inwiefern kann der Mehrwert von Blockchain für die Netzwerkteilnehmer qualitativ beschrieben werden?
3. Welche potenziellen Auswirkungen kann Blockchain auf bestehende Geschäftsmodelle und sozioökonomische Netzwerke haben?

Zeitgleich können diese drei Hauptelemente als Grundlage für die Realisierung eines Blockchain-Anwendungsfalls von der Kernidee, über betriebs- und volkswirtschaftliche Betrachtungen (Mehrwerte für Organisationen und das Ökosystem) bis hin zur Differenzierung zwischen möglichen Ansätzen zur Integration und Erweiterung der Gegenwart gesehen werden (vgl. Abb. 6.1). Dazu lassen sich die im Buch vorgestellten Modelle konkret für die Betrachtungen innerhalb dieser einzelnen Schritte einbinden und als Arbeitsgrundlage verwenden.

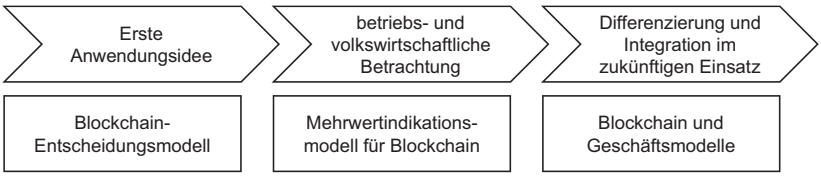

Abb. 6.1 Drei Säulen als Grundlage für die Realisierung eines erfolgreichen Blockchain-Anwendungsfalls – Struktur des Buches. (Eigene Darstellung)

Wie bereits im Buch erwähnt, wird der Blockchain-Technologie das Potenzial zugeschrieben, die Welt grundlegend zu verändern und zu disruptieren. Hierbei ergibt sich eine besonders spannende Fragestellung aus dem Aspekt der Transparenz. Die Transparenz liegt in der Natur der Blockchain, ganz gleich ob es eine permissionless oder permissioned Implementierung ist, auch wenn letztere durchaus keine 100 %ige Transparenz zulässt. Aus diesem Aspekt leitet sich die folgende Frage ab:

Wie wirkt sich die *neue* Transparenz auf das Verhalten von Personen und Organisationen in bisher vorwiegend intransparenten Bereichen aus? Lassen sich Betrug, Manipulation und gezielte Absprachen mittels der Transparenz und Nachvollziehbarkeit präventiv unterbinden? Diese Überlegung lehnt sich an sozialpsychologische Erkenntnisse an, welche belegen, dass allein die Anwesenheit und Beobachtung durch einen Dritten das Verhalten der agierenden Personen bzw. Gruppe oder Organisation beeinflusst [5]. Wenn allen agierenden Akteuren innerhalb eines Netzwerkes bewusst ist,

- dass jede Transaktion vor der Durchführung gegen vorab definierte Geschäftsregeln geprüft wird,
- keine Transaktion im Nachhinein verändert werden kann
- sowie die Transaktionen transparent im Netzwerk geteilt werden,

so ist es denkbar, dass Betrug nicht nur deutlich schwerer wird, sondern allein der Versuch bereits unterbunden und somit das Verhalten nachhaltig positiv beeinflusst werden kann. Ob sich die Welt hierdurch zu einer besseren, faireren oder loyaleren Welt entwickeln lässt, kann nur spekuliert werden. Sicher ist jedoch, dass Blockchain aus technischer Perspektive unser Demokratieverständnis zu einer echten Demokratie entwickeln kann, in welcher alle Entscheidungen auf alle Teilnehmer verteilt werden. Weiter lassen sich Intermediäre in Netzwerken und Prozessen aussparen und Daten zum Allgemeingut machen, wobei der Urheber die volle Kontrolle über Zugriffrechte behält sowie aktiv an der Nutzung seiner Daten partizipieren kann. Zuletzt können auch weniger entwickelte Länder leichter am Fortschritt beteiligt werden, bspw. durch Mikrotransaktionen, -investments oder -kredite.

Literatur

1. FINMA. (2018). *Entwicklungen im Bereich Fintech*. Abgerufen am 13.01.2020 von FINMA: https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/
2. BMWi/BMF. (2019). *Blockchain-Strategie der Bundesregierung: Wir stellen die Weichen für die Token-Ökonomie.* O. O.: BMWi/BMF.

3. Hyperledger Foundation (2017). *Hyperledger Architecture, Volume 1.* o. O.: Hyperledger Foundation.
4. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* o. O.: o. V.
5. Hoppe-Graff, S., & Myers, D. G. (2008). *Psychologie.* Heidelberg: Springer.