

Christiana Köhler-Schute (Hrsg.)

# Blockchains und Distributed-Ledger-Technologien in Unternehmen

Grundlagen, Konzepte und Praxisbeispiele,  
juristische Aspekte



KS-Energy-Verlag

# **Blockchains und Distributed-Ledger-Technologien in Unternehmen**

## **Grundlagen, Konzepte und Praxisbeispiele, juristische Aspekte**

Herausgegeben von

Christiana Köhler-Schute

Mit Beiträgen von

Lumir Boureau, compacer GmbH; Dr. Jens Eckhardt, Derra, Meyer & Partner Rechtsanwälte PartGmbH; Rahman Fakhani, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft; Dr. Zoltan Fazekas, iteratec GmbH; Alexander Elenga Gärtner, IAV GmbH Ingenieurgesellschaft Auto und Verkehr; Sören Högel, WSW Wuppertaler Stadtwerke GmbH; Timm Kellermann, Consulting4Drive GmbH; Johannes Kirchhofer, AdNovum Informatik AG; Sascha Krauskopf, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft; Elke Kunde, IBM Deutschland GmbH; Dieter Rehfeld, regio iT GmbH; Dr. Harald Schöning, Software AG; Björn Steffen, IAV GmbH Ingenieurgesellschaft Auto und Verkehr; Andy Völschow, WSW Wuppertaler Stadtwerke GmbH; Thomas Zweifel, AdNovum Informatik AG

---

**KS-Energy-Verlag**

**ISBN 978-3-945622-09-4**

Alle Rechte, auch die des auszugsweisen Nachdrucks, vorbehalten  
KS-Energy-Verlag, Berlin 2019

Titelfoto: ©Jac - Fotolia.com  
Umschlag: Urs Karl – Mediengestaltung, Berkheim  
Druck: Scandinavian Book, Dänemark

## Vorwort

Bislang wurde das Thema Blockchain durch öffentliche permissionless Blockchains insbesondere im Umfeld von Kryptowährungen geprägt. Mittlerweile stoßen Distributed-Ledger-Technologien (DLT) und mit ihnen Blockchains, als eine Ausprägung von DLT, in Unternehmen auf großes Interesse. Gartner zählt die Technologien zu den zehn wichtigsten Trends für 2019<sup>1</sup>. Auch wenn die ersten Anwendungen im Einsatz sind, der Markt für DLT für den unternehmerischen Einsatz ist noch recht jung und die Umsetzung in Unternehmen erfolgt eher zögerlich. Die Gründe dafür sind vielfältig: Es fehlt u. a. an geeigneten Use oder Business Cases, das Verständnis für die Komplexität der Blockchain<sup>2</sup> – um nur einige Herausforderungen zu nennen. IDC erwartet, dass die Ausgaben für Blockchain im Prognosezeitraum 2018-2022 mit einer durchschnittlichen Wachstumsrate (CAGR) von 76,0% für fünf Jahre und Gesamtausgaben von 12,4 Milliarden US-Dollar im Jahr 2022 wachsen werden. In 2019 liegen die Ausgaben in den USA bei 1,1 Milliarden Dollar, gefolgt von Westeuropa (674 Millionen Dollar) und China (319 Millionen Dollar).<sup>3</sup> Folgt man den Prognosen von Gartner, ist mit der Etablierung vieler Modelle eher mittelfristig zu rechnen.

Bevor man überhaupt in Betracht zieht, ob der Einsatz für das Unternehmen sinnvoll sein könnte, bedarf es eines Grundverständnisses dieser Technologien, zumal der Wissensstand in den Unternehmen sehr unterschiedlich ist. Zur Bewertung von Einsatzmöglichkeiten sollten die unterschiedlichen Ausprägungen der Blockchain bekannt sein und die Weiterentwicklungen der Distributed-Ledger-Technologien im Auge behalten werden. In diesem Buch werden die Grundlagen und Funktionen der Technologie beschrieben und Lösungen wie z. B. Corda, Ethereum, Hyperledger Fabric etc. mit ihren unterschiedlichen Ausprägungen sowie weitere Distributed-Ledger-Technologien wie z. B. IOTA oder Hedera Hashgraph dargestellt.

Im Kontext mit der zunehmenden Digitalisierung und Vernetzung von Unternehmen entstehen branchenübergreifende und interdisziplinäre Kooperationen, um

---

<sup>1</sup> Gartner: Hype Cycle for Emerging Technologies, 2018

<sup>2</sup> Bitkom-Studie: Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen, 2019

<sup>3</sup> <https://www.idc.com/getdoc.jsp?containerId=prUS44898819>, Worldwide Blockchain Spending Forecast to Reach \$2.9 Billion in 2019, According to New IDC Spending Guide, Pressemitteilung vom 4.3.2019

den eigenen Wertschöpfungsanteil zu steigern und neue Geschäftsmodelle zu etablieren. Hier bieten sich private Distributed-Ledger-Technologien als dezentrale Systeme und vertrauenswürdige und sichere Instanzen an, in denen die Partner bzw. Teilnehmer in der Regel bekannt und ihre Rechte definiert sind.

Aber für welche Anwendungsfälle ist der Einsatz einer Blockchain-Lösung sinnvoll oder bieten sich doch etablierte zentrale Lösungen eher an? Welche Vorteile bieten die Technologien und wo liegen ihre Grenzen? Wie sieht die weitere Entwicklung aus? Mit diesen Fragen beschäftigen sich die Autoren und stellen Vorgehensweisen vor, die zur Entscheidungsfindung und Umsetzung in Unternehmen beitragen. Sie stellen Anwendungsszenarien und Pilotprojekte in den unterschiedlichen Branchen vor, gehen vertiefend auf die Entscheidungsfindung in der Automobil- und Mobilitätsindustrie ein und erläutern die von ihren Unternehmen produktiv gesetzten Blockchain-Anwendungen in der Energiewirtschaft (Online-Marktplatz für Strom) und im Einzelhandel (Supply Chain).

Mit der Diskussion über Blockchain stellen sich immer wieder Fragen zu rechtlichen Aspekten, insbesondere hinsichtlich des Datenschutzes, aber auch zivil-, straf- und urheberrechtliche Aspekte gilt es zu berücksichtigen. Hier besteht einiges an Klärungs- und Anpassungsbedarf.

Ziel dieses Buches ist, dem Leser die noch junge Technologie für den unternehmerischen Einsatz greifbarer zu machen und ihm Diskussions- und Planungspunkte sowie hilfreiche Informationen an die Hand zu geben und praxisorientierte Optionen aufzuzeigen. Alle Beiträge sind auch ohne tiefergreifende Programmier- oder Datenbankkenntnisse verständlich und nachvollziehbar.

Zur Zielgruppe dieser Fachpublikation zählen Manager, Praktiker und Berater, Mitglieder von Verbänden und Institutionen sowie Dozierende und Studierende mit der Ausrichtung Digitale Wirtschaft.

An dieser Stelle bedanke ich mich bei den hochkarätigen Experten, die mit ihrem Engagement und ihren informativen Ausführungen zum Gelingen dieses Buches beigetragen haben. Die Autoren stehen dem interessierten Leser für Fragen und Anregungen zur Verfügung.

Christiana Köhler-Schute

Berlin, im September 2019

## Inhaltsverzeichnis

<b>Vorwort .....</b>	<b>5</b>
<b>Management Abstract .....</b>	<b>14</b>
<b>Vom Außenseiter zum Technologie-Standard.....</b>	<b>20</b>
<b>Lumir Boureau</b>	
1 Einführung .....	20
2 Next-Level-Technologie.....	21
3 Dimensionen der Blockchain.....	21
4 Blockchain – Entwicklungsland Deutschland .....	22
5 Wo die Reise hingehet .....	23
<b>Distributed-Ledger-Technologien und Blockchain als Grundlage digitaler Geschäftsmodelle.....</b>	<b>24</b>
<b>Sascha Krauskopf und Rahman Fakhani</b>	
1 Distributed-Ledger-Technologien .....	24
1.1 Ausgangslage und Inhalt des Artikels.....	24
1.2 Grundlegende Funktionsweise und Nutzungsmodelle der DLT. ....	25
2 Blockchain als Ausprägung der Distributed-Ledger-Technologie .....	26
2.1 Eine Einführung .....	26
2.2 Wichtige Bestandteile einer Blockchain als Grundlage für ihre Anwendung .....	28
2.3 Grundkonzept und Funktionsweise der Blockchain.....	29
2.4 Verfügbare Blockchain-Plattformen im Überblick .....	30
2.5 Vor- und Nachteile der Blockchain .....	31
2.6 Grundlegende Anwendungsfelder .....	34
<b>Blockchain und Distributed Ledgers – Grundlagen, Technologien, Funktionsweisen.....</b>	<b>38</b>
<b>Dr. Zoltan Fazekas</b>	
1 Einführung .....	38
2 Dezentrale Buchführung.....	39
3 Allgemeine Grundlagen und ihre Funktionsweise in konkreten DLTs ....	41
3.1 Nodes – Bausteine eines Peer-to-Peer-Netzwerkes .....	41
3.2 States – eine redundant verteilte Datenbank der Wahrheit .....	44

## Inhaltsverzeichnis

3.3	Transaktionen – der Grund laufender Erweiterungen .....	46
3.4	Smart Contracts – automatisierte, selbstausführende Verträge .....	50
3.5	Consensus – der Weg zu konsistenten Datenkopien .....	54
4	Byzantinische Fehlertoleranz – Erreichen des Consensus bei Störungen .....	56
4.1	Consensus in permissioned Netzwerken .....	59
4.2	Consensus in permissionless Netzwerken .....	61
4.3	DLTs mit eigenen Consensus-Mechanismen .....	63
5	Die langsamste Datenbank der Welt .....	66
6	Sicherheit durch kryptographische Verfahren .....	67
7	Unveränderbare Transaktionshistorie .....	69
8	Kombination aus Kryptographie und Spieltheorie .....	72
9	Zusammenfassung .....	74
	<b>Das Hyperledger-Projekt der Linux Foundation .....</b>	<b>77</b>
	<b>Elke Kunde</b>	
1	Blockchain for Business .....	77
1.1	Was ist Blockchain? .....	77
2	Der Bedarf an Blockchain for Business .....	79
3	IBM und Blockchain .....	81
4	Das Open-Source-Projekt Hyperledger .....	83
4.1	Die Hyperledger Frameworks .....	84
4.2	Die Hyperledger Tools .....	86
	<b>Digitale Transformation: Wie die Blockchain das gegenseitige Vertrauen in einem Ökosystem fördert .....</b>	<b>88</b>
	<b>Johannes Kirchhofer und Thomas Zweifel</b>	
1	Einführung .....	88
2	Wachsende Datenmengen: Versionierung, Eigentum, Verantwortung ...	89
3	Eine gemeinsame zentrale Plattform ohne Vertrauen? .....	90
4	Vertrauen ist gut, Kontrolle ist besser: eine verteilte Plattform .....	90
5	Permissioned vs. public .....	91
6	Coopetition: Win-Win-Situation für alle Teilnehmer .....	92
7	Distributed Ledger Technology: eine einmalige Chance .....	93
	<b>Government Blockchain – Basis neuer Geschäftsmodelle .....</b>	<b>94</b>
	<b>Dieter Rehfeld</b>	
1	Blockchain-Initiativen im politischen Umfeld .....	94

2	Blockchain im öffentlichen Sektor .....	96
3	Anwendungsfälle in der öffentlichen Verwaltung und in öffentlichen Unternehmen .....	97

**Die Antwort ist Blockchain – was ist die Frage?..... 100**

**Dr. Harald Schöning**

1	Einführung .....	100
2	Die Idee von „Satoshi Nakamoto“ .....	100
3	Blockchain ist nicht immer die richtige Antwort .....	103
4	Über den Tellerrand hinaus .....	106
5	Fazit .....	108

**Anwendungsfälle: Smart Cities und e-Government ..... 110**

**Sascha Krauskopf und Rahman Fakhani**

1	Blockchain-Geschäftsmodelle im Überblick: Rahmenbedingungen und Vorgehen .....	110
2	Anwendungsfall Smart City: Elemente zur Entwicklung einer sicheren und digitalen Stadt .....	112
2.1	Herausforderung .....	112
2.2	Beschreibung Lösungsansatz – Einsatz der Blockchain bei der Mobilität der Zukunft .....	113
2.3	Beschreibung Lösungsansatz – Einsatz der Blockchain für eine Digitalisierung des Staates: e-Government .....	115
2.4	Beispiele aus der Praxis .....	116
2.5	Möglichkeit der Geschäftsmodellentwicklung anhand von Praxisbeispielen auf Basis Business Model Canvas .....	120
2.6	Grundlegende Kriterien zum Einsatz einer Blockchain und entsprechende Alternativen .....	121
2.7	Alternativen und Weiterentwicklungen auf Basis der Blockchain.....	123
3	Fazit, Handlungsempfehlungen und Ausblick .....	124

**Auf dem Weg durch den digitalen Dschungel: ein strategischer  
Entscheidungspfad für Distributed-Ledger- & Blockchain-  
Technologien in der Automobil- und Mobilitätsindustrie..... 127**

**Timm Kellermann, Björn Steffen und**

**Alexander Elenga Gärtner**

1	Auf einen Blick.....	127
2	Zielsetzung .....	127
3	Übersicht der Anwendungsfälle Auto-Mobilität .....	127

4	Antizipiertes Transaktionsvolumen vs. Latenzanforderung.....	130
5	Experteneinschätzung von DL/BC-Nutzenpotenzial für Auto-Mobilität.	132
6	Klassifizierung von DL/BC-Technologien .....	133
7	Bewertungskriterien zur Eignungsanalyse .....	135
8	DL/BC-Entscheidungsbaum .....	137
9	Wirtschaftlichkeit, Corporate Synergy & CO2-Footprint.....	140
10	Ausgewählte DL/BC-Aktivitäten in der Auto-Mobilität .....	143
11	Strategische Roadmap Distributed Ledger / Blockchain .....	147

**Blockchain meets Reality – der Tal.Markt als Anwendungsbeispiel für die Energiewirtschaft..... 150**

**Sören Högel und Andy Völschow**

1	Die Blockchain – eine anwendungsbezogene Sicht .....	150
1.1	Blockchain.....	150
1.2	Konsensmechanismus.....	151
1.3	Kryptowährung.....	151
2	Die Herausforderungen in der Energiewirtschaft .....	152
3	Der Tal.Markt – der regionale Ökostrommarktplatz .....	153
3.1	Der Endkunde .....	154
3.2	Der Produzent von erneuerbaren Energien (EE) .....	155
3.3	Der Intermediär und die Blockchain als Instrument der Zielerreichung .....	155
4	BlockWerke als Skalierungsmodell .....	156
5	Zusammenfassung und Ausblick .....	158

**Blockchain-Lösungen in Produktion – Beispiel IBM Food Trust ..... 159**

**Elke Kunde**

1	Einführung .....	159
1.1	Blockchain – Hype oder Realität?.....	159
1.2	Hyperledger – Blockchain for Business .....	159
1.3	Produktive IBM-Blockchain-Lösungen Stand Mai 2019 ...	160
2	IBM Food Trust für die sichere Lebensmittelkette.....	161
2.1	Entwicklungsgeschichte und Motivation für diese Lösung	162
2.2	Module der IBM-Food-Trust-Lösung.....	163
2.3	Technologische Aspekte der IBM-Food-Trust-Lösung .....	169
2.4	Nutzen der Lösung.....	171

<b>Distributed Ledger Technology und Blockchain: mehr Rechtsfragen als Antworten? .....</b>	<b>173</b>
<b>Dr. Jens Eckhardt</b>	
1 Einführung .....	173
2 Grundlegende Fragen .....	176
2.1 Recht an der Blockchain als solcher (Urheberrecht, Computerprogramm, Datenbank...) .....	177
2.2 Zivilrechtliche Aspekte .....	179
2.3 Beweiswert einer Blockchain im Rechtsstreit .....	181
2.4 Datenschutzrecht .....	183
3 Einzelrechtsthemen .....	190
3.1 Strafrechtliche Relevanz der Blockchain .....	190
3.2 Verantwortlichkeit des einzelnen Knotenbetreibers.....	190

## Management Abstract

In seinem einführenden Beitrag gibt **Lumir Boureanu**, compacer, einen kurzen Überblick über die Funktionsweise, über Chancen und Grenzen der Blockchain-Technologie und geht auf die Situation in Deutschland ein. Trotz des von Anwenderseite erkannten Potenzials, so der Autor, „steckt die Blockchain in Deutschland noch in den Kinderschuhen“.

**Sascha Krauskopf** und **Rahman Fakhani**, Ernst & Young, erläutern in ihrem Beitrag **Distributed-Ledger-Technologien und Blockchain als Grundlage digitaler Geschäftsmodelle** die Bedeutung von Distributed-Ledger-Technologien (DLT) und Blockchain im Zusammenhang mit der Digitalisierung und insbesondere mit dem Internet der Dinge (IoT) und Industrie 4.0. Sie gehen auf die vier verschiedenen Konstellationen für dezentrale Systeme ein (privat, öffentlich, zugangsbeschränkt, offen) und geben einen Überblick über verfügbare Plattformen der Blockchain (z. B. Ethereum, Hyperledger und Multichain). Sie erläutern die Vor- und Nachteile der Technologie und beschreiben exemplarische Anwendungsfelder für Blockchains, die sich weniger auf Kryptowährungen denn auf unternehmensweite und behördliche Anwendungsfälle beziehen.

**Dr. Zoltan Fazekas**, iteratec, gibt in seinem Beitrag **Blockchain und Distributed Ledgers – Grundlagen, Technologien, Funktionsweisen** zunächst einleitend einen Überblick über den Status quo und die technologische Entwicklung von Distributed Ledgers. Er beschreibt fundiert die Grundlagen und Konzepte von DLTs und Blockchains an den Beispielen Corda, Ethereum und Hyperledger Fabric, ergänzt um IOTA und Hedera Hashgraph. Er erläutert das Grundkonzept von DLTs anhand der Kriterien: Nodes, State, Transaktion, Smart Contracts und Consensus und erklärt detailliert die spezifischen Ausprägungen der genannten Systeme. Am historischen Beispiel der Angriffsplanung autonomer byzantinischer Generäle verdeutlicht er anschaulich die Probleme der Konsensfindung dezentraler Systeme (in diesem Fall autonome Generäle und ihre Truppen) und weist durch Algorithmen erzeugte Lösungswege in permissioned und permissionless Netzwerken auf. Er diskutiert das Dilemma der drei konkurrierenden Eigenschaften von DLTs, das der Dezentralisierung, Skalierung und Sicherheit, für das, so der Autor, „der heilige Gral noch nicht gefunden worden ist.“ Zum Schluss erläutert er Techniken der Kryptographie (Hashfunktionen und digitale Signaturen) und gibt einen Überblick über ausgewählte Prinzipien aus der

gen ist, so **Dr. Harald Schöning**, Software AG, in seinem Beitrag **Die Antwort ist Blockchain – was ist die Frage?** Er wirft Fragen auf, mit denen Unternehmensverantwortliche sich vor dem Einsatz von Blockchains unbedingt auseinandersetzen sollten. Ausgehend von der Ursprungsidee von Satoshi Nakamoto definiert er die Eigenschaften der Blockchain als einer Kombination aus dezentraler Datenhaltung, Anonymität, Integritätsprüfung, Irreversibilität, Unbestreitbarkeit, Konsensbildung ohne vertrauenswürdigen Dritten und geht der Frage nach, wenn auf einige dieser genannten Eigenschaften verzichtet werden kann, ob dann die Blockchain die richtige Lösung ist. Sein erstes Fazit lautet: Innerhalb einer Organisation oder eines Netzwerks, in dem die einzelnen Teilnehmer einander vertrauen, ist der Einsatz von Blockchain nicht erforderlich. Des Weiteren geht er auf Problematiken wie beispielsweise Skalierbarkeit, Sicherheit, Zukunftsfestigkeit etc. ein.

**Sascha Krauskopf** und **Rahman Fakhani**, Ernst & Young, diskutieren in ihrem Beitrag **Anwendungsfälle: Smart Cities und e-Government** die Potenziale der Blockchain-Technologie in Bezug auf die Herausforderungen, potenzielle Lösungen für definierte Problem- bzw. Aufgabenstellungen und beschreiben Beispiele aus der Praxis. Die Beispiele beziehen sich im Mobilitätsbereich auf u.a. Car Sharing, Ladeinfrastruktur (Elektroautos) und Car eWallet, und im Bereich e-Government auf Transparenz und Bürgernähe (digitale Identitäten etc.). Sie erörtern in einem Überblick die Möglichkeit der Geschäftsmodellentwicklung in Bezug auf Smart Cities und Supply Chain auf Basis der Methode Business Model Canvas. Um erste Einschätzungen vorzunehmen, ob der Einsatz von Blockchain sinnvoll ist, haben sie einen geclusterten Fragebogen erstellt, der sich an grundlegenden Kriterien wie z. B. Transparenz, Effizienz etc. orientiert. Im Rahmen eines PoC oder Minimum Viable Products (MVP), so die Autoren, kann der konkrete Nutzen weiter eruiert werden. Sie gehen auf technologische Weiterentwicklungen auf Basis der Blockchain ein, die die Nachteile der Blockchain (z. B. Effizienz) ins Visier nehmen. Zum Schluss erläutern die Autoren zusammenfassend die Problematiken und den möglichen zukünftigen Einsatz von DLTs im unternehmerischen Umfeld und empfehlen, vor Einführung der Blockchain-Technologie eine SWOT-Analyse durchzuführen.

**Timm Kellermann**, Consulting4Drive, **Björn Steffen** und **Alexander Elenka Gärtner**, beide IAV, stellen in ihrem Beitrag **Auf dem Weg durch den digitalen Dschungel: ein strategischer Entscheidungspfad für Distributed-Ledger- & Blockchain-Technologien in der Automobil- und Mobilitätsindustrie** eine Vorgehensweise vor, die auf Basis ihrer durchgeführten Projekte eine Bewertung des Blockchain-Einsatzes im Unternehmen ermöglicht. Zunächst geben sie, entlang eines Aktivitäten-basierten Phasenmodells, einen Überblick über mögliche

Anwendungsfälle und ordnen diese den zwei Dimensionen antizipiertes Transaktionsvolumen und akzeptable Latenzzeit zu, um erste Erkenntnisse darüber zu gewinnen, ob mit den aktuellen Technologien die Anwendungsfälle plausibel darstellbar sind. In einem weiteren Schritt gruppieren und klassifizieren sie Distributed-Ledger- und Blockchain-Technologien nach Merkmalen und Ausprägungen, um sie zu analysieren und mithilfe eines Entscheidungsbaums die Anwendungsfälle den grundsätzlich technischen Eignungskategorien „keine Blockchain“, „Blockchain-Variation“ und „an Blockchain angelehnte Protokolle“ zuzuordnen. Als ergänzende Komponenten für eine abschließende Empfehlung ziehen sie die Bewertung der Wirtschaftlichkeit, die Einbindung in die Corporate Strategy und die Auswirkungen auf den CO2-Footprint hinzu. Sie kommen zu dem Ergebnis, dass aus heutiger Sicht die Transformation auf die DLT-Technologie in der Automobil- und Mobilitätsindustrie nur dann sinnvoll ist, wenn sie elementarer Teil der Unternehmensstrategie ist. Dass und wie viele Akteure die Markteintrittsbarrieren überwinden wollen, veranschaulichen sie an 13 Branchenbeispielen. Um Marktchancen frühzeitig zu adressieren, empfehlen sie PoC und Pilotprojekte. Zur Projektvorgehensweise geben sie Hinweise, die auf ihren Erfahrungen basieren.

Die produktiv gesetzte Anwendung, die **Sören Högel** und **Andy Völschow**, Wuppertaler Stadtwerke, in ihrem Beitrag **Blockchain meets Reality – der Tal.Markt als Anwendungsbeispiel für die Energiewirtschaft** vorstellen, besteht aus der Tal.Markt-Lösung als Marktplatz im Stromsegment für Stromkunden und regionale Produzenten von erneuerbaren Energien und BlockWerke als konsortial-basierte Hyperledger-Fabric-Lösung zur Gewährleistung der Skalierbarkeit und ökonomischen Tragfähigkeit des Geschäftsmodells. Die Tal.Markt-Lösung im Frontend beruht nicht auf ein Peer-to-Peer-Netzwerk. Die Wuppertaler Stadtwerke wickeln als Intermediär die komplexen energiewirtschaftlichen Prozesse wie beispielsweise das Bilanzkreismanagement, den intelligenten wettbewerblichen Messstellenbetrieb etc. und klassische Vertragsdienstleistungen ab. Zwischen dem Endkundenportal und der Blockchain übernimmt eine Softwarekomponente die energiewirtschaftlichen und regulatorischen Aufgaben. Die Motivation der Stadtwerke, diese Lösungen umzusetzen, lag darin, die Commodity-Falle im Stromsegment zu meiden, den Kundenbedürfnissen gerecht zu werden und um mögliche weitere Geschäftsmodelle wie z. B. Elektromobilität etc. auch im Verbund mit geringem zusätzlichem Aufwand abbilden zu können.

**Elke Kunde**, IBM, gibt in ihrem Beitrag **Blockchain-Lösungen in Produktion – Beispiel IBM Food Trust** zunächst einen kurzen Überblick über produktiv gesetzte und in Planung befindliche Blockchain-Anwendungen der IBM, um

dann die IBM-Food-Trust-Lösung vorzustellen. Es geht um eine sichere Lebensmittelkette, die Lebensmittel vom Erzeuger bis zur Filiale im Verbund verfolgbar macht. Sie beschreibt die Probleme, die in der Nahrungsmittelkette auftreten, und das Problembewusstsein und die Motivation vom US-amerikanischen Einzelhandelskonzern Walmart. Nach einigen Pilotprojekten wurde die Food-Trust-Lösung mit Walmart und anderen Kooperationspartnern getestet und ist als Software-as-a-Service-Lösung seit Herbst 2018 in der IBM-Cloud verfügbar. Sie beschreibt die Funktionen der einzelnen Module, angefangen vom Hochladen der Daten, entweder manuell oder über APIs aus vorhandenen Datenquellen, mit ihren Berechtigungsstufen über die Nachverfolgung der Nahrungsmittel, Herkunft, Standort und Status, über Zertifikate, z. B. Betriebserlaubnisse, bis hin zur Datenaggregation mit ihren Auswertungsmöglichkeiten. Sie erläutert die technischen Aspekte der Lösung und erklärt in diesem Zusammenhang die Aufgaben von Trust Anchors und Endorsers und Optionen zur Anbindung an unternehmensinterne Systeme oder an das von Drittparteien. Zum Schluss fasst sie den Nutzen dieser Blockchain-Lösung zusammen.

Der Rechtsanwalt **Dr. Jens Eckhardt** schickt im abschließenden Beitrag **Distributed Ledger Technology und Blockchain: mehr Rechtsfragen als Antworten?** voraus: „Auch wenn derzeit für DLT und Blockchain noch nicht alle Rechtsfragen geklärt sind, ist es bei unternehmerischer Nutzung dieser Technologien geboten, sich auch die Unklarheiten deutlich zu machen, um verantwortungsvolle unternehmerische Entscheidungen treffen zu können.“ Für die rechtliche Bewertung ist entscheidend, so der Autor, dass es nicht die eine Distributed-Ledger-Technologie gibt. „Für die juristische Bewertung ist die konkrete Ausgestaltung entscheidend.“ Zunächst geht er der grundsätzlichen Frage nach, wer eigentlich Rechte an einer Blockchain hat und wer z. B. im Fall einer Anfechtung in die Verantwortung genommen werden kann. Im Zusammenhang mit zivilrechtlichen Aspekten erläutert er z. B. Verstöße gegen das Bürgerliche Gesetzbuch und die Einordnung und Bewertung von Smart Contracts. Er erläutert die Risiken hinsichtlich des Beweiswertes von Digitalisaten (z. B. gescannte Urkunden / Originaldokumente), diskutiert, wie pseudonymisierte Daten im Zusammenhang mit der DS-GVO zu bewerten sind und wer die Verantwortung für die Einhaltung des Datenschutzes in einer public und private Blockchain trägt. Die Unveränderbarkeit in der Blockchain widerspricht dem Recht auf Löschung persönlicher Daten und Vergessenwerden. Eine Möglichkeit wäre, so der Autor, ältere Blöcke aus der Blockchain zu entfernen, welches in einer großen public Blockchain wie Bitcoin nicht, in einer private Blockchain hingegen theoretisch schon möglich wäre. Allerdings würde dies einen gravierenden Vorteil der Blockchain, nämlich den der Unveränderbarkeit, untergraben. Des Weiteren erläutert er die technischen Maßnahmen, die nach der DS-GVO zu berücksichtigen sind, wenn es um die

Verarbeitung von personenbezogenen Daten geht. Zum Schluss thematisiert er die Verantwortlichkeit eines einzelnen Knotenbetreibers bei straf- oder urheberrechtlichen Verstößen.

# **Blockchain und Distributed Ledgers – Grundlagen, Technologien, Funktionsweisen**

**Dr. Zoltan Fazekas**

## **1 Einführung**

Die anfängliche Euphorie bzgl. Blockchain ist im Jahr 2018 allmählich in tiefe Ernüchterung umgeschlagen. Die einstigen Phantasien, was man mit einer manipulationssicheren Datenbank in der Welt verbessern könnte, sind skeptischen Fragen nach realen Anwendungsfällen und tragfähigen Geschäftsmodellen gewichen. Um diese zu beantworten, muss man Geschäftsmodelle ideologisch neu denken: weg von traditionellen hin zu kooperativen Geschäftsmodellen, in denen man gleichzeitig Mitgestalter, Miteigentümer und Nutznießer ist und nicht nur notwendige Ressource oder Einnahmequelle eines Unternehmens im Mittelpunkt des Geschäftsmodells. Es entstehen offene Ökosysteme mit dezentralisierter Governance, die nicht von einer zentralen Autorität, sondern von der gesamten Community bestimmt werden. Blockchains und Distributed-Ledger-Technologien (DLT) kommen dabei eine wichtige Rolle zu.

Seit der Erfindung von Bitcoin sind über 10 Jahre vergangen und man ist in dieser Zeit technologisch weit gekommen. Viele Probleme blieben dennoch bis heute ungelöst. In den letzten Jahren war vor allem die Skalierung der Haupttreiber der technologischen Entwicklung. Neben Layer 1-Lösungen wie Sharding und Layer 2-Lösungen wie State Channels und Side Chains wurden auch neue DLTs wie Hashgraph und IOTA mit innovativen, aber in der Praxis noch zu wenig erprobten Consensus-Algorithmen entwickelt. Um bessere Skalierung zu ermöglichen, wird auch eine bereits etablierte Technologie wie Ethereum komplett überarbeitet und neben anderen Features um Proof of Stake als Consensus ergänzt. Projekte wie Cosmos und Polkadot gehen einen Schritt weiter und verfolgen das Ziel, ein interoperables Netzwerk von Blockchains zu ermöglichen. Obgleich sich manche Technologien annähern, wie etwa Hyperledger Fabric durch die Unterstützung seiner Smart Contracts an Ethereum, ist eine Konvergenz bzw. Konsolidierung am Markt noch nicht festzustellen. Eine gemeinsame Basis, unter anderem bzgl. der Terminologie, ist allerdings unerlässlich, um die wachsende Vielfalt an Technologien vernünftig analysieren und vergleichen zu können. Hier können internationale Standards wie die Spezifikationen der Enterprise Ethereum Alliance

oder die geplanten Normen der ISO/TC 307 Blockchain und Distributed Ledger Technologies weiterhelfen.

## **2 Dezentrale Buchführung**

Das Cambridge Dictionary definiert den Begriff Ledger als „a book in which things are regularly recorded, especially business activities and money received or paid“. Das Führen von lückenlosen Aufzeichnungen ist notwendig, um die Ordnungsmäßigkeit einer Geschäftsaktivität nachzuweisen. Wenn alle Aktivitäten an einer zentralen Stelle geprüft und erfasst werden, kann man etwaige Unregelmäßigkeiten erkennen. Da mehrere Organisationen in der Geschäftsaktivität involviert sind, kann entweder jede von ihnen ihre eigenen Aufzeichnungen führen oder sie können diese Aufgabe einer der beteiligten Organisationen oder einem unbeteiligten Dritten, einem vertrauenswürdigen Mittelsmann, überlassen. Alle drei Möglichkeiten haben ihre Nachteile, die am Ende des Tages in zusätzlichen Kosten münden: für den regelmäßigen Abgleich der parallel geführten Schattenaufzeichnungen zur Bereinigung etwaiger Inkonsistenzen oder für die Dienste der mit der Führung der Aufzeichnungen beauftragten Organisation. Die Höhe dieser Kosten ist tendenziell steigend, da Angriffe von außen durch immer mehr Schutzmaßnahmen und Manipulation innerhalb des Systems durch zunehmend verschärfte Compliance-Maßnahmen abgewehrt werden müssen. Die damit gewonnene Sicherheit ist auf der anderen Seite nur begrenzt, wie zahlreiche erfolgreiche Hacker-Angriffe und Betrugs-Skandale der Vergangenheit zeigen.

Gibt es eine effizientere und sicherere Alternative, als jemand anderem die volle Kontrolle und Verantwortung zu übertragen? Könnten die notwendigen Prüfungen und Aufzeichnungen von denjenigen, die an den Geschäftsvorgängen beteiligt sind, gemeinsam geleistet werden? Könnte man sicherstellen, dass alle die eigene Aufgabe ordnungsgemäß durchführen und keiner das Ergebnis manipuliert, ohne den anderen Beteiligten vertrauen zu müssen? Distributed Ledgers sind die Antwort auf diese Fragen. Es gibt sie in vielen Ausprägungen. Einige nutzen eine Datenstruktur, die als Blockchain bekannt ist. Blockchains sind somit eine Teilmenge von DLTs. Der Einfachheit halber wird in den nächsten Kapiteln die Abkürzung DLT verwendet, die auch die Blockchain subsumiert. Nur bei Aussagen, die sich spezifisch auf die Blockchain und keine anderen DLTs beziehen, wird der Begriff Blockchain genutzt.

In den nachfolgenden Kapiteln wird der Versuch unternommen, die gemeinsamen Prinzipien aller DLTs technisch fundiert zu erklären. Es ist eine Herausforderung, dies auf wenigen Seiten unterzubringen, da DLTs komplex und im Detail auch sehr unterschiedlich sind. Sich auf eine Technologie zu beschränken

und nur diese vorzustellen, wird der Sache aber nicht gerecht. Eine abstrakte Darstellung der Gemeinsamkeiten ohne spezifische Details einzelner DLTs ebenso nicht. Es werden stattdessen die Technologien möglichst breit und tief beleuchtet und durch konkrete Beispiele gezeigt, wie unterschiedlich die gemeinsamen Grundkonzepte umgesetzt werden können. Bei der Wahl der Technologien wurde nicht nur ihre aktuelle Bekanntheit berücksichtigt. Die Entscheidung fiel auf Technologien, an denen man die Unterschiede zwischen Blockchains und anderen DLTs oder zwischen permissionless und permissioned Netzwerken am besten veranschaulichen kann. Ein weiteres Kriterium war die universelle Einsetzbarkeit. Im Gegensatz zu Bitcoin und anderen DLTs, die nur Zahlungen unterstützen, sollten die ausgewählten Technologien ein breites Spektrum an dezentralisierten Anwendungen ermöglichen. Aus diesen Gründen fiel die Wahl auf **Ethereum**, **Hyperledger Fabric** und **Corda**, ergänzt um **IOTA** und **Hedera Hashgraph**, die in einem eigenen Kapitel über alternative Consensus-Mechanismen vorgestellt werden. Es wird bewusst auf die Präsentation von Hintergrundinformationen über die Entstehungsgeschichte, Persönlichkeiten, Organisationen sowie aktuelle Kennzahlen hinter den einzelnen Technologien verzichtet (s. dazu auch die nachfolgenden Beiträge). Stattdessen liegt das Augenmerk auf der Erklärung der Konzepte und ihrer Funktionsweise.

Als roten Faden haben wir die gemeinsamen Grundkonzepte (vgl. Tabelle 2) gewählt, die DLTs in irgendeiner Form aufweisen: Nodes, State, Transaktionen, Smart Contracts<sup>10</sup> und Consensus. In jedem Kapitel beginnen wir die Erklärung eines dieser Konzepte auf einer höheren Abstraktionsebene, um die Gemeinsamkeiten aller DLTs für den Leser erkennbar zu machen, und weisen dann anhand der ausgewählten Technologien auf die unterschiedlichen Ausprägungen hin. Nach der Vorstellung der fünf Grundkonzepte befassen wir uns in den restlichen Kapiteln mit den theoretischen Grundlagen – von der Funktionsweise verteilter Netzwerke über Kryptographie bis hin zur Spieltheorie – und ihrer Anwendung in DLTs.

Kommen Ihnen manche der Überschriften der nachfolgenden Kapitel bekannt vor? Wir haben uns populärer Aussagen bzw. Antworten auf die Frage, was eine Blockchain oder DLT ausmacht, bedient. Jede einzelne dieser Aussagen ist rich-

---

<sup>10</sup> Nicht alle DLTs unterstützen frei programmierbare Smart Contracts. Zum Beispiel sind in Bitcoin Transaktionen nur Skripte zur Prüfung der benötigten Signaturen und anderer einfacher Bedingungen vorgesehen. Auch NEM und IOTA unterstützen keine Smart Contracts. Bei Werttransfer-Transaktionen prüfen sie jedoch automatisch die ausreichende Verfügbarkeit der Werte, damit Empfänger nur so viel erhalten können, wie die Sender ausgeben können.

tig, stellt aber nur einen Aspekt der Technologie dar. Erst zusammen mit den anderen ergibt sich ein Gesamtbild, das die Funktionsweise von DLTs begreifbar macht.

Wir unternehmen bewusst nicht den Versuch, die englischsprachigen Begriffe, mit Ausnahme dem der „Transaktion“, zu übersetzen. Da der Großteil der Literatur und Dokumentation von DLTs nur in englischer Sprache verfügbar ist, würde eine Übersetzung lediglich die Zuordenbarkeit der Begriffe und die Verständlichkeit der nachfolgenden Kapitel erschweren.

Node	Computer zum Speichern von States und Verarbeiten von Transaktionen im Einklang mit Smart Contracts und dem Consensus
State	Daten über die aktuelle gemeinsame Sicht aller User
Transaction	Befehle von Usern zur Aktualisierung der States
Smart Contract	Regeln bzgl. der Zulässigkeit von Transaktionen
Consensus	Regeln bzgl. der Reihenfolge von Transaktionen

Tabelle 2: Grundlegende Konzepte einer DLT

### 3 Allgemeine Grundlagen und ihre Funktionsweise in konkreten DLTs

#### 3.1 Nodes – Bausteine eines Peer-to-Peer-Netzwerkes

Jede DLT basiert auf einem Netzwerk von Computern, die in der Regel als **Node** bezeichnet werden. Auf den Nodes läuft eine Software<sup>11</sup>, die für die Kommunikation mit anderen Nodes im Netzwerk verantwortlich ist. Weitere Aufgaben dieser Software umfassen die Speicherung der States, das Empfangen und Weiterleiten von Transaktionen, die Ausführung von Smart Contracts und die Aktualisierung des State anhand der Transaktionen, die nach den Regeln des Consensus akzeptiert wurden. Wir erklären die in Tabelle 2 dargestellten Zusammenhänge und Aufgaben eines Nodes ausführlich in den nächsten Kapiteln.

---

<sup>11</sup> In Ethereum wird die Software auf den Nodes, leider etwas irreführend, Client genannt.