

**Michael Merz**

# **Blockchain im B2B-Einsatz**



**Michael Merz**

# **Blockchain im B2B-Einsatz**

**Technologien, Anwendungen und Projekte**



PUBLISHING

### **Impressum**

Texte: © Copyright by Dr. Michael Merz  
Verlag: MM Publishing  
C/O PONTON GmbH  
Dorotheenstr. 64  
22301 Hamburg  
info@mm-publishing.de  
Umschlagfoto: © Copyright by Frank Fox  
Coverdesign: Deborah Klein, [www.deborahklein.de](http://www.deborahklein.de)  
Buchsatz: BookDesigns, Potsdam  
Druck: MegaDruck.de  
ISBN: 978-3-9820560-1-2

Das Werk, einschließlich seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung des Autors unzulässig. Dies gilt insbesondere für die elektronische oder sonstige Vervielfältigung, Übersetzung, Verbreitung und öffentliche Zugänglichmachung.

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

# ■ Inhaltsübersicht

<b>Prolog</b>	<b>1</b>
<b>1 Vorwort</b>	<b>3</b>
<b>2 Hype oder Hoffnung?</b>	<b>11</b>
2.1 Blockchain als Dotcom-Blase 2.0?	11
2.2 Die zehn größten Blockchain-Mythen	16
<b>3 Wie funktioniert die Blockchain?</b>	<b>23</b>
3.1 Die Blockchain als verteiltes System	24
3.1.1 Austausch von Transaktionen	31
3.1.2 Blockbildung	35
3.1.3 Trustlessness	40
3.1.4 Wer bildet den nächsten Block?	41
3.1.5 Soft Forks: Die Chain am Scheideweg	46
3.1.6 Finderlohn für neue Blöcke	48
3.1.7 Proof of Work, Proof of Stake, Proof of Authority	51
3.1.8 Inhalt der Blockchain	55
3.2 Smart Contracts	59
3.2.1 Ethereum als Smart-Contract-Mutterschiff	62
3.2.2 Ethereum Token	66
3.2.3 Code is Law	68
3.2.4 Dapps – Distributed Applications	70
3.2.5 Einschränkungen der Ethereum-Blockchain	74
3.2.6 Kryptofinanzierung und die „Tokenization“ von Geschäften	82

## ■ Inhaltsübersicht

3.3	Weitere Blockchain-Technologien	91
3.3.1	Tendermint	92
3.3.2	Hyperledger	102
3.3.3	BigchainDB	108
3.3.4	IOTA – Blockchain ohne Chain und ohne Blöcke	111
3.3.5	Hedera Hashgraph	117
3.4	Was braucht die Blockchain der Zukunft noch?	118
3.5	Standardisierung von Blockchain-Technologie	134
3.6	Die Blockchain-Technologie passend zur Anwendung auswählen	140
3.7	Zusammenfassung und Definition: Was macht eine Blockchain aus?	145
<b>4</b>	<b>Einsatzpotenziale der Blockchain in der Energiewirtschaft</b>	<b>147</b>
4.1	Energiehandel und -transport heute	147
4.2	Aktuelle und zukünftige Entwicklungen im Strommarkt	155
4.3	Einsatz der Blockchain im Energiehandel	161
4.3.1	Status quo 2018: Blockchain und Energie	162
4.3.2	Szenario 2022: Evolutionärer Einsatz der Blockchain	163
4.4	Szenario 2030: Ein perfekter Energiemarkt?	173
4.4.1	Nutzung eines Smart Market	177
4.4.2	Die unsichtbare Hand des Netzbetreibers	179
4.4.3	Handelnde Parteien am Strommarkt im Jahre 2030	181
4.5	Nutzung der Blockchain in Energiemärkten	187
<b>5</b>	<b>Organisatorische Herausforderungen bei B2B-Blockchains</b>	<b>191</b>
5.1	Beispiele für den disruptiven Einsatz der Blockchain	194
5.1.1	Beispiel: Rohstoffbörse	195
5.1.2	Beispiel: Versicherungen ohne Versicherer	198
5.2	Wenn der Fahrstuhl zur Achterbahn wird	203
5.3	Blockchain-Governance	206
5.4	Finanzierung eines Blockchain-Projekts	210

<b>6</b>	<b>Blockchain in der Energiewirtschaft – Projektbeispiele</b>	<b>215</b>
6.1	Enerchain	217
6.2	NEW 4.0	227
6.3	Handel zwischen Prosumenten und Konsumenten	232
6.3.1	Stufe 2016: „Ethical Trading“	235
6.3.2	Stufe 2019: Zuteilung mit Abrechnung durch den Lieferanten	235
6.3.3	Stufe 2021: ETIBLOGG	240
6.4	Gridchain	242
6.5	StromDAO	248
6.6	Auf der Suche nach der Weltformel des Energiehandels	250
<b>7</b>	<b>Das WRMHL-Framework</b>	<b>253</b>
7.1	Referenzarchitektur für verteilte Anwendungen	253
7.2	WRMHL	256
7.3	Synchronisierte verteilte Anwendungen für Konsortien	269
<b>8</b>	<b>Finale Gedanken</b>	<b>273</b>
	<b>Glossar</b>	<b>277</b>
	<b>Index</b>	<b>285</b>
	<b>Abbildungsverzeichnis</b>	<b>291</b>
	<b>Tabellenverzeichnis</b>	<b>295</b>
	<b>Literaturverzeichnis</b>	<b>297</b>



## ■ Prolog

75XBOBBY99-----6 wollte gerade eine Abkürzung nach Wacken nehmen, als ihn ein Konvoi anderer RoboCars blockierte. Er hatte nicht erwartet, dass so viele RoboCars, sogar aus Flensburg, hierher kamen – das konnte ihm an diesem Morgen tatsächlich noch den Ladeslot vermasseln.

Sieben Monate lag sein ICO bereits zurück, und seit vier Monaten fuhr 75XBOBBY99-----6 nun mehrmals in der Woche nach Wacken. Seine Holder hatten mit ihm bereits einen guten Schnitt gemacht. Insgesamt waren es 476 Accounts. Manchmal verkaufte einer, manchmal kam einer hinzu – aber alles in allem handelte es sich um einen recht ruhigen Kreis von Investoren. 75XBOBBY99-----6s Marktkapitalisierung lag bei 2.365 Enercoins – für ein sieben Monate altes RoboCar nicht phänomenal, aber doch ganz okay.

Seinen Owner hatte er am Morgen beim Zahnarzt abgeliefert. Der Termin war allerdings auf 9:00 Uhr angesetzt, sodass 75XBOBBY99-----6 aufgrund dieser späteren Zeit eine andere Route nach Wacken gewählt hatte. Trotz der Entfernung von Hamburg, war Wacken am Morgen der beste Ort zum Laden, denn der Strom sollte dort den ganzen Tag kostenlos sein. In der Nacht hatte es gestürmt, daher waren auch die allerletzten Bleibatterien in der Region randvoll aufgeladen. Alle Elektrolyseure in der Region liefen bereits auf Hochtouren und bis Mittag waren noch fünf Windstärken aus Nordwest angesagt.

Einzig diese Kolonne aus Kiel machte ihm einen Strich durch die Rechnung – zu große Nachfrage war Gift für die Preise und 75XBOBBY99-----6 könnte zudem seinen Slot verpassen! Seit ein paar Tagen nutzte er Ladestationen bei einer Windanlage, die sich etwas außerhalb von Wacken befand. Heute jedoch musste er spontan einen neuen Ladeslot reservieren, denn der Zahnarzttermin war ungeplant dazwischengekommen. Zum Glück hatte er seinen ursprünglichen Slot für 7:50 Uhr intraday mit geringem Verlust an 75XXXJULIAD7SK7G verkaufen können.

Für 75XBOBBY99-----6 war das oberste Ziel, seinen Holdern eine vernünftige Rendite zu liefern. Dazu gehörten auch Entscheidungen wie an diesem Morgen: kurzfristig noch Slots handeln und dabei möglichst viele Enercoins einsammeln. Und dann eben etwas weiterfahren, um dort die Batterien aufzuladen. Direktes Anzapfen der Windanlagen bot den großen Vorteil, dass der Strom zu minimalen Preisen bezogen werden konnte – also kein Netznutzungsentgelt, keine Umlagen, nur Mehrwertsteuer auf fast nichts. Dafür hatte sich 75XBOBBY99-----6 sogar kürzlich seine Batterie aufstocken lassen.

Früher mussten die Windanlagen immer abgeschaltet werden, wenn sie zu viel produzierten – „Einspeisemanagement“ nannten sie dies damals voller Euphemismus. Eigentlich hätte

## ■ Prolog

man diese Maßnahme „Kapitalvernichtung“ nennen sollen. Der Strom konnte damals nicht durch die Netze abtransportiert werden, sie waren einfach nicht auf eine dezentrale Stromproduktion ausgelegt. Man hatte lange überlegt, ob die Netze ausgebaut werden sollten, allerdings hätte dies zig Millionen Enercoins gekostet (damals, in der Zeit der Fiat-Währungen, waren dies über 50 Milliarden Euro). Aber warum stattdessen nicht die Batterien zu den Engpässen bringen, wo auch immer sie auftraten? Autos standen doch die meiste Zeit untätig herum! Insofern schlug sich jede Änderung der Wetterprognose heute sofort als Änderung des Straßenverkehrs nieder. Man konnte die Uhr danach stellen: Sobald eine aktualisierte Wetterprognose Wind über 20 km/h ankündigte, waren die Autobahnen keine zehn Minuten später in Richtung Küste verstopft.

Die wenigen Menschen, die noch selbst fuhren, hatten sich daher daran gewöhnt, überall im Stau leere RoboCars um sich zu sehen, wenn diese sich wie eine Lawine aufs Land wälzten. Anfangs hatte man tatsächlich überlegt, Plastikpuppen auf dem Fahrersitz aufzublasen, damit Menschen sich auf den Straßen nicht zu verlassen fühlten, aber nachdem RoboCars irgendwann auch keine Fahrersitze mehr hatten, wurde die Idee ad acta gelegt.

Inzwischen hatte 75XBOBBY99-----6 Wacken rechtzeitig erreicht. Er dockte an einer Dose an und verweilte hier für vier Stunden. Der Strom reichte bis zum Wochenende, und im Laufe des Tages konnte er noch ein paar bezahlte Fahrten machen, bis er gegen 18:00 Uhr seinen Owner wieder vom Büro abholen würde.

## ■ 1. Vorwort

Blockchain! Man mag es fast schon nicht mehr hören, so sehr reden alle von einer Technologie, die häufig missverstanden, überhöht und gleichzeitig unterschätzt wird. Schon vor einigen Jahren begann sich die internationale Blockchain-Community von der Nerd- und Kryptoszene hin zu Anwendungsfeldern in der Finanzbranche, der Energiewirtschaft und vielen anderen Branchen zu erweitern. Damit einher ging eine immer weiter steigende Überhöhung der Technologie.

Die Blockchain wurde als Problemlöser für einfach alles propagiert – am besten noch mit einer Beimischung von künstlicher Intelligenz und Big Data. Da sich dies bereits seit Jahren immer weiter verstärkte, unternahm ich vor einigen Monaten den Versuch, das Phänomen „Blockchain“ aus einer möglichst neutralen, agnostischen Perspektive zu beschreiben und die Möglichkeiten und Grenzen der Technologie aufzuzeigen. Daraus entstand schließlich dieses Buch.

Es findet sich im Internet bereits eine große Zahl an Quellen zum Thema, anhand derer man sich eine gute Wissensgrundlage erarbeiten kann. Zudem finden in jeder größeren Stadt regelmäßig Konferenzen statt und YouTube ist überfüllt mit Videos, die erklären, wie die Blockchain funktioniert. Warum dann noch ein weiteres Buch zu diesem Thema schreiben?

Dieses Buch trägt den Titel „Blockchain im B2B-Einsatz“ – dies bedeutet einerseits, dass wir uns mit dem Thema „Blockchain“ *aus technischer Sicht* beschäftigen. Andererseits analysieren wir die *B2B*-Prozesse einer Branche, um konkret zu veranschaulichen, welche Einsatzmöglichkeiten bestehen, und was dabei im Detail zu beachten ist. Die Energiewirtschaft dient hier lediglich als Platzhalter für viele weitere Branchen, in denen Geschäftsprozesse ablaufen, die eine große Zahl Geschäftspartner umfassen. Anhand von Projektbeispielen soll schließlich gezeigt werden, welche Prozesse sich warum besonders gut durch die Blockchain unterstützen lassen.

Eine ganzheitliche Betrachtung von der Technologie bis hin zur Anwendung, wird dem Leser dabei behilflich sein, basierend auf Erfahrungen mit Konsortien wie Enerchain, NEW 4.0, Gridchain, oder ETIBLOGG einen Schritt weiter zu gehen und aus diesen Projekten und Erfahrungen zu lernen.

### Zur Einordnung

Ich habe also dieses Buch geschrieben, weil die Nische „Blockchain im B2B-Einsatz“ noch kaum mit Praxisbeispielen besetzt ist. Zugegebenermaßen ist es auch eine schwierige Nische, denn zwischen Schreibtischarbeit, schnell programmierten Smart Contracts und tatsächlichem Betrieb liegen Welten, gerade im Bereich „Blockchain“. Dazu kommt, dass der produktive Betrieb gerade erst beginnt.

Die bereits bestehende Vielzahl an Blockchain-Büchern erklärt das Thema entweder eher technisch oder auf der Ebene von „Managementliteratur“. Jeder Autor hat dabei seine eigene Perspektive auf das Thema. Es ist wie das gute alte Beispiel des Elefanten im dunklen Raum, den mehrere Personen befühlen und zu beschreiben versuchen: er ist gleichzeitig Gartenschlauch, Flügel, Kordel, Baumstumpf, Dolch, Lederwand, etc. Auch viele Buchautoren nähern sich der Blockchain aus unterschiedlichen Perspektiven: es gibt sehr gute Bücher, die sich äußerst detailliert bis auf Programmcode-Ebene mit den vielen Fragestellungen rund um Bitcoin beschäftigen. Die Bücher von Andreas Antonopoulos (z.B. [Anto17]) benutze ich selbst zum Nachschlagen, wenn ich wirklich alle Details von Bitcoin verstehen will. Wer mag, kann sich per „Managementliteratur“ á la Tapscott & Tapscott [TaTa16] einen Überblick verschaffen. Viele weitere Publikationen beleuchten detailliert das Thema „Blockchain“ aus zusätzlichen Perspektiven – sie betonen das Disruptionspotenzial oder neue Möglichkeiten für die Gesellschaft, Prozesse dezentral zu denken. Wiederum andere setzen einen Schwerpunkt im Bereich innovativer Geschäftsprozesse und zählen dazu gängige Beispiele auf (elektronisches Grundbuch, Chargenrückverfolgbarkeit in der Lieferkette, Nachhaltigkeitszertifizierung bei der Herstellung von Konsumprodukten, etc.). Dabei ist häufig der technische Teil verkürzt und man verliert das Gefühl dafür, ob diese Prozesse denn wirklich unter Berücksichtigung aller realen Umstände umsetzbar sind. Einen Prototyp zu programmieren und eine Blockchain live zu nutzen liegen im Aufwand Größenordnungen voneinander entfernt. Wichtig ist daher bei Blockchain-Prozessen, die Verbindung zwischen Anwendung und Technologie herzustellen und immer wieder deren Zusammenwirken zu hinterfragen, denn die harten Herausforderungen zeigen sich erst beim Endspurt.

Es gibt noch einen weiteren Blickwinkel auf das Thema „Blockchain“, nämlich den des Zweiflers. Ein solches Buch möchte ich an dieser Stelle ebenfalls empfehlen, weil gerne in der Community ignoriert wird, dass der Einsatz der Blockchain nicht immer Sinn macht: „Attack of the 50 foot blockchain“ von David Gerard [Gera17]. David habe ich auf einer Konferenz in London erlebt und er hat dort vieles, was die Krypto-Szene zu bieten hat – von Bitcoin über Smart-Contracts, DAOs, ICOs bis hin zu B2B-Blockchains – als, höflich ausgedrückt, noch sehr frühreif entlarvt. In seinem Buch legt er bei einer großen Zahl an Unzulänglichkeiten, Problemen, Missverständnissen, Verklärungen, Verwirrungen und Skandalen den Finger in die Wunde. David ist also ein ausgewiesener Blockchain-Contrarian und es war sehr anregend, mit ihm zu debattieren. Wenn Sie also ein überzeugter Blockchain-Enthusiast sind, ertragen Sie bitte unbedingt auch Davids Buch und erden Sie sich! Es nützt niemandem, von einem Einsatz der Technologie zu träumen, bei dem wichtige Eigenschaften vernachlässigt werden und deren Prinzip dann keinen Mehrwert stiften kann – das Ergebnis wäre im Zweifel nur „money down the drain“.

## Warum also dieses Buch?

Wenn Sie trotz der 50-Fuss-Blockchain immer noch Interesse haben, dieses Buch zu lesen – was kann ich Ihnen bieten? Das Anliegen dieses Buches ist, entsprechend Abbildung 1 eine Fahrstuhlfahrt durchzuführen – aus den Kellern der Technik in die Vorstandsetage und wieder zurück. Und wieder hinauf und zurück, und dies noch ein paar weitere Male. „Blockchain“ kann am besten verstanden werden, wenn der Leser beide Ebenen kennt und sich oben wie unten zuhause fühlt. Dann macht die Fahrstuhlfahrt Spaß und man gerät in den „Flow“, etwas ganz Neues zu designen. Diese Fahrstuhlfahrt im B2B-Umfeld zu machen, konfrontiert uns immer wieder mit der Situation, alte Geschäftsprozesse in einem neuen Licht zu betrachten oder sogar neue Prozesse zu entwerfen, die das alte Rollengefüge durcheinanderwirbeln können. Da dies eine inspirierende Tätigkeit ist, liegt der Fokus dieses Buches auf dem Einsatz der Blockchain im B2B-Umfeld.

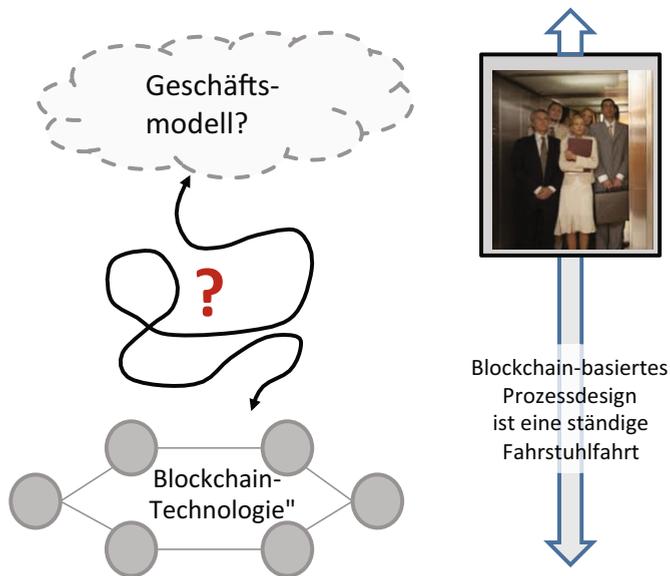


Abbildung 1: Blockchain-Projekte erfordern regelmäßige Perspektivenwechsel

Mit diesem Buch möchte ich also das Wagnis eingehen, ganz unterschiedliche Themenschwerpunkte gleichzeitig zu beleuchten. Es soll die Technik, aber auch die Anwendung abgedeckt werden. Da mein Unternehmen speziell für die Energiebranche tätig ist, möge der Leser es mir nachsehen, dass ich den fachlichen Schwerpunkt genau dort setze. Dies hilft hoffentlich auch Energie-Laien, das Für und Wider innerhalb dieses Anwendungskontextes zu verstehen und auf Prozesse im eigenen Umfeld zu übertragen.

Ich habe darüber hinaus auch versucht, andere Projekte, in die wir nicht selbst involviert sind, für dieses Buch aufzubereiten, jedoch bestand in den meisten Fällen das Problem,

dass man jenseits des Marketingschleiers kaum an Detailinformation gelangen konnte. Oft endeten diese Projekte auch in einer frühen Prototypphase. Insofern geht mein Dank an die Protagonisten von StromDAO, mit denen ich in einem sehr detaillierten Gespräch ein tieferes Verständnis für ihre Technologie entwickeln konnte. Sollten sich in dieser Hinsicht in Zukunft weitere Details zu anderen Projekten ergeben, werde ich selbstverständlich in späteren Auflagen solche Projekte in das Kapitel 6 aufnehmen.

Das Themenfeld „Blockchain“ ist heute inzwischen so weit ausdifferenziert, dass dieses Buch Fragestellungen zu den unterschiedlichsten Kryptowährungen weitgehend ausklammert. Man könnte hier die Besonderheiten von DASH, Zcash, NEO etc. erörtern, sowie über deren Historie, Tools und Handelsmöglichkeiten diskutieren oder darüber was einem Kryptoinvestor bei der Nutzung alles widerfahren kann. Hierzu finden sich interessante Publikationen wie z.B. [Köni17] oder [Berg18]. Ebenso stehen Fragestellungen zu Kryptobörsen, die Investition in Token, ICOs, oder Entscheidungshilfen zum Mining in diesem Buch nicht im Vordergrund.

## Blockchain im B2B-Einsatz

Ich verstehe unter einer *B2B-Blockchain* eine Integrationstechnologie, die speziell auf die Anforderung von Industriekonsortien ausgerichtet ist und dafür Blockchain-Mechanismen wie Immutabilität, Konsensbildung, 1:N-Kommunikation, Redundanz auf Basis preiswerter, Knoten usw. für eine effiziente Koordination einsetzt.

B2B-Blockchains bieten damit die Möglichkeit, bestehende Geschäftsprozesse zu optimieren oder abzulösen. Dementsprechend disruptiv ist der Einfluss auf die Organisation des geschäftlichen Miteinanders. Blockchain-Projekte in der Industrie finden allerdings häufig hinter verschlossenen Türen statt – lautes Marketing ist daher über Branchengrenzen hinaus nicht nötig. Das Ziel liegt bei solchen Projekten in der Optimierung von Prozessen und nicht in der breiten Publikation der Ergebnisse.

Industriekonsortien finden sich jedoch immer wieder mit ähnlichen Fragestellungen konfrontiert, egal, welcher Branche sie angehören: „Passt ‚Blockchain‘ zu unserem Geschäftsprozess?“, „Ist es sinnvoll, unseren Prozess an die Blockchain anzupassen?“ oder „Können wir möglicherweise einen ganz anderen Prozess finden, der das Potenzial der Blockchain viel besser nutzt?“. Und dann entstehen weitere Fragen: „Wie wollen wir die Blockchain organisieren?“, „Wie wollen wir uns selbst organisieren?“, „Wieviel Zentralisierung brauchen wir am Ende doch noch, ohne durch die Hintertür in die Welt der alten Prozesse zurückzufallen?“. „Was sagt der Regulator, was der Gesetzgeber zu unserem Ansatz?“, „Wie können wir verhindern, dass sich durch die Hintertür ein (neuer) Monopolist einschleicht?“, „Wer steht beim neuen Prozess auf der Verlierer- und wer auf der Gewinnerseite?“ – Fragen über Fragen!

Anhand der Projektbeispiele aus der Energiewirtschaft und speziell des Energiehandels sollen solche Fragen exemplarisch in diesem Buch beleuchtet werden.

## Was ist das Problem für die Lösung?

Eine Schwierigkeit bei Blockchain-Projekten liegt in der unterschiedlichen Verteilung von Expertenwissen. Wer ein Blockchain-Projekt durchführen will, muss die Technologie verstehen *und* den umzusetzenden Prozess. Dies ist jedoch kein lineares Vorgehen, sondern erfordert einen regelmäßigen Perspektivenwechsel. Mal ist die Technologie Ausgangspunkt der Betrachtung: „Wie können wir die hohe Verfügbarkeit, Trustlessness und niedrigere Betriebskosten zu unserem Vorteil nutzen?“ Mal stehen fachliche Anforderungen im Vordergrund: „Wie kann ich Kunden am Prozess teilnehmen lassen, ohne mit der Datenschutzgesetzgebung in Konflikt zu geraten?“

Bei „klassischen“ IT-Projekten steht der „Business Case“ im eigenen Unternehmen als Treiber einer Entwicklung im Vordergrund. Eine neue Lösung ist zu implementieren, ein Prozess effizienter zu gestalten, eine Anwendung zu entwickeln, die neuen externen oder internen Anforderungen genügen soll. Daraus leiten sich ein Plan und eine Spezifikation ab, die per „Wasserfall“ oder iterativ umgesetzt wird. Tools und Verfahren werden so ausgesucht, dass die zu entwickelnde Software bestmöglich die Anforderungen erfüllt. Natürlich werden bei diesen „klassischen“ Projekten auch für die Betriebsphase die entsprechenden Leistungsanforderungen so umgesetzt, dass eine höchstmögliche Qualität erreicht wird. Alles „in time, in budget, in quality“ – natürlich wie immer... In jedem Fall aber folgt die Lösung der Problemstellung.

Und nun ist da diese Blockchain-Technologie! Alle wollen etwas mit ihr entwickeln und einmal ausprobieren, ob sich das Ziel nicht auch mit dieser neuen Technologie schneller, besser, disruptiver erreichen lässt. Das Management will verkünden, dass auch das eigene Unternehmen „Blockchain“ kann. IT-Kollegen wollen mit der Technologie spielen und ihre Möglichkeiten ausprobieren, andere sehen eine Möglichkeit, ihren Lebenslauf mit einem attraktiven Thema anzureichern.

Aber die Blockchain hat ein Problem: sie ist technisch nicht besonders anpassungsfähig. Im Gegensatz zu einer SQL-Datenbank ist ihr technischer Spielraum recht begrenzt. Sie ist ja noch nicht einmal eine Datenbank! Und schützenswerte Daten lassen sich auch nicht ohne weiteres in ihr speichern. Und dann ist da auch noch die Wartezeit bis zum Konsens, bzw. die Frage, wo denn überhaupt die vielen Knoten installiert werden sollen – und warum das alles, wenn doch eigentlich nur die gute alte Vereinsverwaltung auf einen neuen Stand gebracht werden soll?

Es wäre daher technisch sinnlos, für die Entwicklung einer Vereinsverwaltung die Blockchain einfach unter das klassische Anwendungsdesign zu „flanschen“. Dies macht vielleicht zu Marketingzwecken Sinn, doch der für den Systembetrieb verantwortliche Administrator würde wohl sofort kündigen. Also bleibt es bei einem Prototyp, mit dem man aber wenigstens noch eine Blockchain-betriebene Vereinsverwaltung vorweisen und durch diesen Innovationsnachweis die Marktkapitalisierung des eigenen Unternehmens erhöhen kann ...

Die Blockchain ist also keine Lösung für eine Riesenzahl an Problemen.

## ■ Vorwort

Eine tatsächlich sinnvolle Blockchain-Anwendung zu entwickeln, ist reichlich schwieriger: sie ist eher die Antwort auf eine Frage, die erst noch formuliert werden muss. Sie ist eine Lösung für ein Problem, das noch gar nicht festgestellt wurde. Man muss in vielen Fällen sogar das Geschäftsmodell aus den Möglichkeiten und Einschränkungen der Blockchain ableiten. Und noch schwieriger: man muss die Plattform des eigenen Unternehmens verlassen, um aus der Helikopter-Perspektive nach Einsatzmöglichkeiten zu suchen. Es muss folglich akzeptiert werden, dass das eigene Unternehmen nur ein Rädchen im Getriebe des zukünftigen Prozesses sein wird. Man sollte also besser Volkswirt als Betriebswirt sein, um den globalen Nutzen der Technologie zu entdecken.

Dies wiederum erfordert umso mehr die enge Zusammenarbeit zwischen technischen Blockchain-Experten und geschäftlichen Innovatoren, die einander zuhören und gemeinsam Neuland betreten. Ein solches Vorgehen wird häufig von Innovationsmanagern gefordert. Dazu gibt es unzählige Bezeichnungen und Seminare – es ist jedoch kein Spaziergang. Dieses Vorgehen ähnelt eher einer permanenten Fahrstuhlfahrt in den Keller der Kryptografie, über das Parkdeck der verteilten Systeme, die unteren Stockwerke der Unternehmensprozesse, bis zur Chefetage der branchenübergreifenden Veränderung von Prozessen und Märkten. Entsprechend viele Knowhow-Träger sind zu synchronisieren, denn einzelne Personen, die alle Wissensgebiete gleichzeitig beherrschen, sind rar.

## Zum Inhalt

In diesem Buch soll also eine solche Fahrstuhlfahrt über alle relevanten Etagen durchgeführt werden:

- Um „Blockchain“ ranken sich Mythen und Missverständnisse, von denen ich einige in *Kapitel 2* beiseite räumen möchte. Dies macht hoffentlich Appetit auf den Rest des Buches.
- In *Kapitel 3* werden technische Grundlagen vermittelt – teilweise am Beispiel von Bitcoin, denn es ist die Mutter aller Blockchains, die bestverstandene und bestdokumentierte. Teilweise aber auch anhand von Technologien, die für Industriekonsortien relevanter sind.
- Der nichttechnische Schwerpunkt liegt im Bereich der Konsortial-Blockchains. Hier geht es um einige Anwendungsbeispiele, mit denen sich Industriekonsortien heute und in Zukunft befassen. Um diese Anwendungsfälle besser im Kontext einer speziellen Branche zu verstehen, gibt *Kapitel 4* einen ausführlichen Überblick zum heutigen Energiehandel, und wie dieser sich im Rahmen der Energiewende langfristig verändern wird.
- Nachdem das Spektrum der Fahrstuhlfahrt zwischen technologischer Lösung und den Anforderungen, die sich aus dem Wandel der Energiebranche ergeben, abgesteckt ist, wird in *Kapitel 5* untersucht, wie unternehmensübergreifende Prozesse mit der Block-

chain unterstützt werden können und welche Anforderungen dies an das Konsortium stellt.

- In *Kapitel 6* finden sich einige Blockchain-Projekte aus Forschung und Praxis im Rahmen der Energiewende, die sich in das in Kapitel 4 skizzierte „Szenario 2030“ einfügen.
- *Kapitel 7* zieht Schlüsse aus den technischen und fachlichen Anforderungen und formuliert eine Referenzarchitektur, bei der auch Blockchains im B2B-Einsatz eine Rolle spielen. Schließlich stelle ich das WRMHL-Framework vor, mit dem wir verteilte B2B-Prozesse realisieren.

Ich hoffe, dass der Leser nach Bewältigung dieses Buches mit etwas Rüstzeug ausgestattet ist, um nicht nur die Blockchain-Technologien besser zu verstehen, sondern gleichzeitig auch eine Wahrnehmung für ihre möglichen B2B-Einsatzbereiche und deren Grenzen zu entwickeln. Wer dann in seiner Branche, in seinem Unternehmen oder bei den ihn umgebenden Prozessen zu dem Ergebnis kommt, dass die Blockchain nicht bloß eine Lösung ohne Problem darstellt, sondern eine grundlegende Veränderung seiner Branche herbeiführen kann, macht nicht nur mich als Buchautor glücklich, sondern wird darüber hinaus mit dem Ritterorden der Fahrstuhlführer geehrt!

Wenn dieses Buch also den Leser in die Lage versetzt, in Blockchain-Prozessen zu denken und dabei den erforderlichen Perspektivenwechsel zwischen IT und Geschäftsmodell zu leisten, dann hat es seinen Zweck erfüllt. Ich habe bewusst versucht, den Umfang so knapp zu halten, dass das Buch an einem Wochenende verdaut werden kann. Gleichzeitig hoffe ich, dass die Ganzheitlichkeit des Themas auch durch dieses Buch reflektiert wird, ohne dass es dem Krypto-Freund bei Kapiteln mit Energie-Schwerpunkt langweilig wird, und ohne dass der Anwender beim Lesen der eher technischen Kapitel den Abend durch frühzeitiges Einschlafen beendet.

Da ein Buch heutzutage ein sehr statisches Gebilde ist, habe ich eine Website zum Buch eingerichtet: <http://blockchain-b2b-book.com>. Hier werde ich Informationen und Updates posten, so dass sich der Leser auf dem neuesten Stand halten kann.

Zudem haben wir in den letzten Monaten verschiedene Erklär-Videos zu unterschiedlichen Blockchain-Themen produziert. Diese finden sich in unserem YouTube-Channel, der sich mit den Suchbegriffen „Ponton“, „Blockchain“ und „Channel“ finden lässt.

## Denglisch oder Dscherman?

Kurz noch etwas zur Terminologie: Das Blockchain-Geschäft quillt über vor Anglizismen. Bei „Hash“, „Mining“, „Genesis Block“ oder „Smart Contract“ ist es etablierte Praxis, beim englischen Original zu bleiben. Wenn es elegant und passend klingt, habe ich andere ins Deutsche übersetzt, z.B. „Blockzeit“ und „Knoten“. Für viele andere wiederum würde eine Übersetzung zu gezwungen klingen, z.B. „Wertmarke“ statt „Token“ oder „Nichterfordernis von Vertrauen“ statt „Trustlessness“. Gleiches gilt auch für die energiefachlichen Fragestellungen in den hinteren Kapiteln: Sollte „Smart Meter“ und „Smart Grid“ statt „intelligente

■ Vorwort

Messstelle“ bzw. „intelligentes Netz“ verwendet werden? Insofern führte meine Intuition zu einer Wahl, die begrifflich vielleicht eine andere rote Line zieht zwischen Deutsch und Englisch als bei anderen Autoren. Der Leser möge hier Nachsicht walten lassen! Ich fürchte, die sprachlichen Grauzonen werden noch ein paar Jahre bestehen, bis sich eine einheitliche Blockchain-Sprache etabliert hat.

## Vielen Dank

Natürlich beschert ein Buch dem Autor eine Menge Schreibaarbeit, die auch das persönliche Umfeld in Anspruch nimmt. Bedanken möchte ich mich daher bei meinen Kollegen und Mitarbeitern, deren Rat geholfen hat, das Buch in seiner inhaltlichen Ausrichtung zu fokussieren. Ich möchte auch Frank Fox danken für das Recht, die mikroskopische Aufnahme der Volvox-Algen als Cover-Bild zu verwenden. Ähnlich der Blockchain entstand dezentral organisiertes Leben aus einfachen, autonomen Zellen, die gemeinsam ein Ganzes formen, das auch bei Verlust einzelner Bestandteile überlebensfähig bleibt. Des Weiteren bedanke ich mich bei den vielen Reviewern und Korrekturlesern, die wertvolle Anregungen beigesteuert haben sowie schließlich bei Dilek und Sophie für ihr Verständnis und die Unterstützung dafür, dass ich mich zum Schreiben so manche Woche in Klausur begeben habe.

Hamburg, 3. Januar 2019

## ■ 2. Hype oder Hoffnung?

Warum ist das Thema „Blockchain“ nur so ein Hype? Das letzte Mal habe ich eine solche Überhöhung eines technischen Themas Ende der 90er Jahre erlebt – damals ging es um das Internet im Allgemeinen und speziell um „E-Commerce“ mit all seinen technischen und organisatorischen Ausgestaltungen: Über das Internet bezahlen, ein Ladengeschäft online eröffnen, ohne Regeln und Einschränkungen, die einem Unternehmer in der Ladenpassage einer Kleinstadt das Leben erschweren würden. Das wäre etwas! Die späten 90er waren voller Technik-Visionen, die zum größten Teil Geschäftsmodelle des heutigen Internet vorwegnahmen. Es war die Rede vom „Long Boom“ – einem Wirtschaftswachstum, dessen Ende einfach nicht absehbar war, es gab massenweise IPOs (Initial Public Offerings, d.h. Börsengänge junger Startup-Unternehmen) auf den Marktsegmenten der Börsen, die auf junge Technologieunternehmen ausgerichtet waren (in Deutschland war dies der Neue Markt). Auf diesen waren die Regeln so abgeschwächt, dass ein Startup mit wenigen Mitarbeitern, wenigen Monaten Erfahrung, aber großen Visionen binnen kürzester Zeit Millionen DM einsammeln konnte.

### 2.1 Blockchain als Dotcom-Blase 2.0?

Während diese Entwicklung des Internet von der Spezifikation des IP-Protokolls bis zum Dotcom-Boom Ende der 90er Jahre etwa 30 Jahre benötigte, erlebten wir in weniger als 10 Jahren ab dem Go-Live der ersten Blockchain, wie sie 2008 im Artikel von Satoshi Nakamoto [Naka08] beschrieben wurde, bis zur heutigen Welt, in der ICOs (Initial Coin Offerings) von Blockchain-Startups Inhalt der Tagespresse sind, eine immer rasantere Entwicklung neuer Sub- und Subsubtechnologien, bei der auch Insider schnell den Überblick verlieren können.

Es gab zudem in den 90ern Bücher wie „Blur“ [DaMe98] die das Verschwimmen alter Grenzen vorweg sahen – Grenzen zwischen Organisationen, zwischen Abteilungen, zwischen Kontinenten und Kulturen zwischen Arbeit und Freizeit, da bereits damals absehbar war, dass das Internet Grenzen auflösen würde und dass jeder Mensch mit jedem anderen in Kontakt treten kann und jeder jederzeit erreichbar ist. Man ging damals von einer vollkommenen Dezentralisierung der Gesellschaft durch das Internet aus. Eine Vision, in der wenige Internet-Konzerne einen großen Teil des Datenverkehrs auf sich zentralisieren würden, war damals unvorstellbar. Es gab damals wie heute Menschen, die sich durch technische Visionen der Dezentralisierung begeistern lassen und voller Erwartung an dieser Zukunft teilhaben wollen.

## ■ Hype oder Hoffnung?

Damals gab es noch keine „Meetups“ zu den vielen, heute viel stärker differenzierten Tech-Themen, aber z.B. „First Tuesday“-Veranstaltungen, bei denen die Gründer-, Nerd-, und Investorenszenen aufeinandertrafen, zu denen sich jeder irgendwie dazuzählte. Und tatsächlich gab es Umschichtungen in Wirtschaft und Gesellschaft: Agfa und Kodak gehören heute der Vergangenheit an<sup>1</sup>. Kinder fragen heute, warum in den alten Filmen immer eine Schnur am Telefon hängt und warum dieses eine Wählscheibe hat und kein Display. Überhaupt ist der Begriff „Wählscheibe“ bei vielen Menschen selbst aus dem passiven Wortschatz verschwunden. Im technischen Umfeld drehte sich ebenfalls alles um „E-Commerce“, der ab Mitte der 90er zum Hype-Thema wurde. *XML* (eXtensible Markup Language) zum Beispiel wurde als E-Commerce-Technologie verstanden und vermarktet. Es war tatsächlich ein „Enabler“, der es Unternehmen ermöglichte, strukturiert und standardisiert Daten auszutauschen. Aber XML wurde maßlos überhöht: ich selbst durfte im Jahr 2000 auf dem Schloss Fuschl im Salzburger Land aus ganz Europa zusammengetrommelten Journalisten im Rahmen einer Expertenrunde erklären, warum XML und das veranstaltende Unternehmen, das XML für sich als E-Commerce-Technologie und Marketing Message entdeckt hatte, die nächsten 100 Jahre fundamental durcheinander wirbeln würde. Naja, mein Beitrag setzte sich zusammen aus solch nüchternen Technologie-Versatzstücken wie „verteilte Systeme“, „B2B-Integration“ und „typischere Validierung von XML-Schemata“. Konsequentermaßen schielten daher die meisten Zuhörer gelangweilt und mit knurrendem Magen zum Buffet hinüber ...

## Hauptsache „Blockchain“

Die Parallelen zu heute sind aber deutlich: wieder gibt es den Kreis der Technikbegeisterten, die sich auf eine neue, noch nicht vollständig verstandene Technologie stürzen. Wieder leben wir in einer Zeit, in der wir erwarten, dass es nur darauf hinauslaufen kann, mindestens 30 Jahre lang alle Branchen durchzuwirbeln, diesmal eben durch die Blockchain. Wieder verschwimmt in Zukunft alles zu einem Blockchain-Brei – vom Smart Meter über Privatpersonen, RFID-Chips, Geräte, und die wenigen noch verbleibenden Unternehmen, die nicht von Smart Contracts wegdisruptiert werden... Am besten nimmt man dann noch „Artificial Intelligence“, „Internet of Things“ und „Big Data“ dazu, dann kann man ja gar nichts falsch machen – irgendetwas passt davon schon zusammen.

Es ist dabei für Nichttechnologen sehr schwer einzuschätzen, wo die Trennlinie zwischen Wahrheit und Vision verläuft. Und wenn man sich eher der Realität als dem Marketing verpflichtet fühlt, dann ist es umso ärgerlicher, was täglich in der Presse zum Thema „Blockchain“ zu lesen ist.

---

1 Für Kodak gilt dies nun auch wieder nicht ganz: Das Unternehmen, von dem man glaubte, dass es gar nicht mehr existierte, warb Ende 2017 mit der Einführung einer eigenen Blockchain, über die das Rechte-Management für das geistige Eigentum an Fotos durchgeführt werden kann. Nach Bekanntwerden dieser Meldung schoss der Aktienkurs um 120 % in die Höhe.

Der Entschluss, das Thema „Blockchain“ vom persönlichen Interesse zum Schwerpunkt meiner beruflichen Tätigkeit zu wandeln, war konsequenterweise durch eine Pressemitteilung getrieben, die im März 2016 die Runde machte: „Die erste Energiehandelstransaktion über die Blockchain fand im Brooklyn Microgrid statt“<sup>2</sup>. Nicht, dass ich etwas gegen Energiehandelstransaktionen über die Blockchain hätte, nur hätte man „Blockchain“ in solch einer Mitteilung auch durch „MySQL“, „Java“, „COBOL“ oder „Brieftauben“ ersetzen können. Man hätte den Verkauf einer Kilowattstunde (kWh) auf *irgendeine* Weise realisieren können. Aber mit „Blockchain“ hat man das Marketing auf seiner Seite – und zehntausende Blockchain-Fans weltweit, die bei jeder Meldung der Art „Jetzt auch XYZ über die Blockchain“ reflexhaft jubeln. Die technische Charakteristik der Blockchain tritt dabei komplett in den Hintergrund. „Blockchain“ ist häufig zum bloßen Transmissionsriemen verkommen, mit dem man sich weltweit Sichtbarkeit verschaffen kann.

Es gab sogar begeisterte Journalisten, die sich auf die Reise nach New York machten, um sich vor Ort das „Brooklyn Microgrid“ anzusehen. Da war jedoch nichts zu finden! Kein startuppiges Büro mit bunter Spielecke, keine Bevölkerung, die begeistert auf den Straßen Blockchain-Samba tanzte, nicht einmal jemand, der Auskunft geben konnte. Warum auch? Die Blockchain spielt sich im abstrakten Raum ab, nicht in Brooklyn. Und die Handvoll Solarpaneele stehen auf den Dächern, fünf Stockwerke oberhalb der Straßen Brooklyns.

Das Brooklyn Microgrid war aber in der Tat der „Urknall“ für eine Reihe von Projekten im Bereich „Blockchain und Energie“ und somit auch für mich der Anlass, das Thema „Blockchain“ auch in meinem eigenen Unternehmen in die Tat umzusetzen – allerdings wollten wir uns auf das tatsächliche Potenzial der Technologie im B2B-Bereich konzentrieren, und dabei analysieren, wo genau die Möglichkeiten und Grenzen liegen. Wir wollten auch herausfinden, wie man feststellen kann, ob ein Prozess, ein „Business Case“ oder ein Markt Blockchain-affin ist oder eben nicht.

## eCash - Die Mutter aller Kryptowährungen

Zum Glück gab es Vorentwicklungen, die uns dabei behilflich waren, schnell in dieses Thema einzusteigen. Zum einen hatte ich mich zunächst bereits in den 90er Jahren mit der Kryptowährung „eCash“ [Chau82] beschäftigt (siehe oben: alles schon mal da gewesen ...) und dann seit 2011 mit Bitcoin. Außerdem hatte mein Unternehmen bereits seit 2001 einen Schwerpunkt im Bereich B2B-Integration – also in der Unterstützung unternehmensübergreifender Prozesse über das Internet – gesetzt, was eine gute Ausgangslage darstellte.

Im Rahmen meines Promotionsvorhabens in den 90er Jahren ging es um „Elektronische Dienstmärkte“ [Merz99], vereinfacht ausgedrückt also um „E-Commerce“ – und der hatte unter anderem auch mit „Bezahlen“ zu tun. Bezahlen an sich bedeutete auch damals bereits,

---

2 <https://www.newscientist.com/article/2079334-blockchain-based-microgrid-gives-power-to-consumers-in-new-york>

## ■ Hype oder Hoffnung?

ein Bezahlfverfahren einzusetzen, das in der Regel die Übertragung von Kreditkartendaten über das Internet vorsah. Es gab bereits hunderte solcher Verfahren, so wie es heute tausende von Kryptowährungen gibt. Bezahlfverfahren waren jedoch prinzipiell ein eher langweiliges und wenig promotionswürdiges Thema. Dagegen war eCash von ganz anderer Qualität. eCash war eine *Währung*, in der man anhand elektronischer Münzen zahlen konnte – und dies auch noch anonym bzw. nicht rückverfolgbar („untraceable transactions“). eCash hatte im Jahr 1996 weltweit über 30.000 Teilnehmer begeistert, die im Rahmen eines Feldtests ein Wallet installierten und hiermit ein Initialbudget von 100 Cyberbucks erhielten. Es gab keine Möglichkeit, zwischen Fiat-Währungen wie DM oder Dollar auf der einen Seite und Cyberbucks auf der anderen Seite zu tauschen. Die eCash-Ökonomie war quasi abgenabelt und musste eine Eigendynamik entwickeln, Cyberbucks mussten auf andere Weise einen eigenen Wert erlangen. Insofern gab es erste Versuche, für eCash spielerisch etwas Nützliches anzubieten. Die einen hatten einfache digitale Bilder gemalt und gegen eCash verkauft, andere ein Gedicht geschrieben und wiederum andere online um eCash gebettelt – oder einfach eine versprochene Leistung nicht erbracht und die Zahlung eingesteckt.

An der Universität Hamburg hatten wir damals ein Börsenspiel entwickelt, das die 30 DAX-Werte einmal täglich abrief und um den Faktor 100 herunterskalierte. Wenn also der Aktienkurs von Volkswagen bei 50 DM stand, konnte man eine Aktie für 0,50 Cyberbucks kaufen. Da ja Teilnehmer zunächst Aktien bei unserem Server kaufen mussten, bevor sie diese später wieder verkaufen konnten, sammelte sich in unserem Wallet ein beträchtliches Cyberbuck-Vermögen. In Spitzenzeiten nahmen über 2.500 Aktionäre an unserem Börsenspiel teil. Die Begeisterung, eine völlig neue, unabhängige Währung zu schaffen und auszuprobieren, war damals groß. Groß war aber auch die Enttäuschung, dass es mit dem Spiel irgendwann wieder vorbei war. eCash war zu zentralisiert (es gab als „Zentralbank“ den sogenannten Mint-Server, der gleichzeitig auch *Single-Point-of-Control* und damit *Single-Point-of-Failure* war), der kryptografische Aufwand war für damalige Verhältnisse recht hoch. Als dann schließlich die Deutsche Bank eCash in Umlauf bringen wollte, schob die Bundesbank dem Krypto-Treiben einen Riegel vor, denn das Währungsmonopol sah nur einen Herausgeber von „Geld“ vor. Und aufgrund der Zentralisierung von eCash war immer ein „Betreiber“ greifbar und haftbar.

## Von Bitcoin zur Blockchain

Der eCash-Feldversuch verlor sich im weiteren Verlauf der späten 90er Jahre dann in Bedeutungslosigkeit, die sich weiter aufblähende New-Economy Bubble forderte einen 12-Stunden-Tag, und die spätere Gründung unseres Unternehmens ebenfalls. B2B-Themen standen von nun an bei uns im Vordergrund: Supply-Chain-Integration in der Papierindustrie im Rahmen des Projekts „papiNet“, die Datenintegration zwischen Energiehändlern, die sich ihre Trade-Daten per XML-Messaging bestätigten, das regulatorische Reporting von Energiehandelstransaktionen zwischen Teilnehmern am Energiemarkt und den Daten-Reposi-

tories der Regulatoren, sowie eine Kommunikationsinfrastruktur, die den Datenaustausch im Rahmen des Lieferantenwechselprozesses zwischen Netzbetreibern und Stromlieferanten bewältigt. In jedem Fall ging es immer um *Standardisierung*, und die damit verbundene Effizienzsteigerung, die zu Kostensenkung und Risikominderung führte.

Gleichzeitig geschah es im Jahre 2011, dass ich – aufgeschreckt durch die Schockwellen der Finanzkrise – aus privatem Interesse an einer Konferenz zum Thema „Gutes Geld“ teilnahm. Dort begeisterte mich ein Vortrag zur Privatwährung „Mark Banco“<sup>3</sup> mit der Andeutung, dass möglicherweise in einer fernen Zukunft dies auch über das Internet in elektronischer Form möglich sein könnte. Ich schickte einem Bekannten in Holland eine SMS über das Thema „Privatwährungen“ und erhielt als Antwort: „Kennst Du schon Bitcoin?“. Der Rest ist persönliche Geschichte. Ich kaufte mir 50 Bitcoins für 2 Euro je Stück (die ich 2013 leider schon wieder ausgegeben hatte – von Entführungen bitte ich abzusehen!) und verfolgte seitdem die Entwicklung der ersten tatsächlich erfolgreichen Kryptowährung – weniger als „Aktivist“ oder Protagonist, und auch nicht als Softwareentwickler, dazu war ich nicht mehr in der Lage, sondern eher von der Seitenlinie aus. Etwas später entstand die Erkenntnis, dass Bitcoin quasi aus zwei Hälften besteht. Die „obere“ ist die Anwendung „Kryptowährung“, die untere ist „Blockchain“. Doch letztere war bei Bitcoin fest an erstere gekoppelt und damit in ihrer breiteren Nutzung stark eingeschränkt. Befreit von dieser Klammerung versprach jedoch die Blockchain-Technologie schon 2012 sehr viel mehr Potenzial als „nur“ Kryptowährungen zu unterstützen. Mike Hearn, einer der ersten Entwickler, der noch mit Satoshi Nakamoto zusammenarbeitete, wurde bereits 2012 nicht müde, auf die Nutzungsmöglichkeiten von Smart Contracts auf Bitcoin-Basis hinzuweisen – sie waren schließlich sein persönliches Baby.

Es dauerte dann aber noch weitere Jahre, in denen das Thema „Blockchain“ so viel Eigendynamik entwickelte, dass es bald auch in einer größeren Öffentlichkeit als „Enabler“ speziell für B2B-Prozesse erkannt wurde. Damit einher ging eine Wiederholung der späten 90er Jahre: Marketing, Hype, Missverständnisse und überhöhte Erwartungen. Viele sprachen in der Branche bereits vom Handel über die Blockchain und für mich und auch für mein Unternehmen war irgendwann erkennbar, dass wir es bei der Blockchain ebenfalls mit dem Thema „B2B-Integration“ zu tun hatten – mit neuen Mitteln und Möglichkeiten, aber auch mit Restriktionen. Es erforderte jetzt nur noch eines kleinen Anstoßes, die beiden Themen „Blockchain“ und „B2B-Integration“ zusammen zu führen, und dieser Anstoß war dann das Brooklyn Microgrid im März 2016.

---

3 Die Mark Banco war eine seit 1619 von der Hamburger Bank herausgegebene Privatwährung, die durch Edelmetall unterlegt war. Sie wurde aufgrund einer Initiative Hamburger Kaufleute geschaffen, um dem Umlauf gefälschter Münzen anderer Währungen durch eine qualitativ hochwertige Privatwährung zu ergänzen. Im Gegensatz zu vielen Fiat-Währungen endete die Mark Banco nicht in der Inflation oder im Staatsbankrott, sondern wurde 1875 von der Reichsmark abgelöst.

## ■ Hype oder Hoffnung?

Im Anschluss setzte ich mich mit unseren Entwicklern zusammen und wir überlegten, was denn tatsächlich ein aktueller, möglichst disruptiver und zu uns passender Anwendungsfall sein könnte. Es sollte die Autonomie von Marktteilnehmern gefördert werden, der Transaktionsdurchsatz sollte überschaubar bleiben, d.h. wir wollten die noch neue Technologie nicht mit tausenden Transaktionen pro Sekunde belasten, und wir wollten zudem das Disruptionspotenzial der Blockchain demonstrieren. Hieraus entstanden das Enerchain-Projekt<sup>4</sup> (siehe auch Kapitel 6.1) sowie das Buchkapitel „Einsatzpotenziale der Blockchain im Energiehandel“ [Merz16].

Doch bei aller Euphorie sollte man nüchtern bleiben. Es ist mir immer ein Anliegen, darauf hinzuweisen, dass ich grundsätzlich eine Blockchain-agnostische Haltung einnehme. Einerseits fasziniert auch mich diese Technologie und ich glaube ebenfalls an ihr Potenzial, andererseits ist meine Perspektive keineswegs die des Startup-Gründers, der mit seiner Technologie die Welt blockchainifizieren will. Aus meiner Erfahrung als Softwareentwickler und Unternehmer würde ich immer die bestmögliche Lösung für ein Anwendungsproblem suchen. Dies *kann* Blockchain sein – muss aber nicht. Es *kann* Ethereum oder Tendermint oder Hyperledger oder IOTA sein. Oder eine Technologie, die erst noch entwickelt werden muss. Als Entscheidungsträger sollte man hier unbedingt entspannt bleiben. Wie im Kapitel 5 nachzulesen ist, kann man davon ausgehen, dass nur ein kleiner Teil der Geschäftsprozesse, die täglich in einem Unternehmen und um dieses herum ablaufen, überhaupt Blockchain-Kandidaten sind. Aber einige von ihnen besitzen erhebliches Disruptionspotenzial – und genau dies macht diese Technologie so spannend.

## 2.2 Die zehn größten Blockchain-Mythen

Ein Anliegen dieses Buches ist es, das Thema „Blockchain“ zu entmystifizieren. Ich würde mich freuen, wenn Menschen, die einige Wissensfragmente zum Thema aufgeschnappt haben, in Zukunft wenigstens den folgenden zehn Missverständnissen nicht mehr unterliegen würden. Dieses Buch hat seinen Zweck bereits erfüllt, wenn Sie als Leser zu den folgenden Statements wissen, warum diese missverständlich oder falsch sind. Die im Folgenden verwendeten Fachbegriffe werden selbstverständlich weiter hinten im Buch erläutert.

### Missverständnis Nr. 1: „Die Blockchain ist langsam“

Dies ist richtig, es gilt aber vor allem für Bitcoin – und dort sogar in zweierlei Hinsicht: die Blockzeit liegt im Durchschnitt bei 10 Minuten und man sollte in der Regel eine Stunde warten, bis die eigene Transaktion sicher in der Blockchain gespeichert ist. Solche Verzögerungen finden sich nur bei öffentlichen Blockchains. Warum diese Aussage jedoch für Konsortial-Blockchains falsch ist, findet sich weiter hinten in Kapitel 3.

---

<sup>4</sup> <https://www.enerchain.com>

Zudem ist Bitcoin auch langsam, weil traditionell nur bis zu sieben Transaktionen pro Sekunde verarbeitet werden können. Dies ist ein schwacher Wert, der durch eine Flexibilisierung der Blockgröße entspannt werden könnte, wenn es denn die Entwickler-Community nur wollte. Wiederum gilt diese Einschränkung insbesondere für Bitcoin als öffentliche Blockchain – aber eben nicht für das Prinzip der Blockchain im Allgemeinen, siehe hierzu auch Kapitel 3.

## **Missverständnis Nr. 2: „Die Blockchain verbraucht zu viel Energie“**

Auch hier bezieht man sich – ohne es vielleicht zu wissen – auf öffentliche Blockchains wie Bitcoin oder Ethereum, deren Konsensmechanismus auf dem Prinzip „Proof of Work (PoW)“ basiert. Speziell bei Bitcoin liegt der weltweite Energieverbrauch inzwischen bei zwei Atomkraftwerken (ca. zwei Gigawatt), die permanent erforderlich sind, um das sog. Mining mit Strom zu befeuern. Eine Konsortial-Blockchain kann hingegen auf wenige Knoten verteilt werden, die jeweils nur wenige Euro Hosting-Gebühr im Monat kosten. Siehe auch hierzu Kapitel 3.3 zu den speziellen Eigenschaften von Konsortial-Blockchains.

## **Missverständnis Nr. 3: „Die Blockchain ist unsicher“**

Ja, es wurden Börsen ausgeraubt, Bitcoins gestohlen, Waren nicht geliefert, Handelspartner sind nicht identifizierbar oder befinden sich in einem Land mit zweifelhafter Rechtsprechung, etc. Aber hier finden Raub und Betrug *auf der Anwendungsebene* oder sogar auf der Ebene der Web-Front-Ends statt – und dies eben wieder bei Bitcoin, Ethereum et al. Wie gesagt, Kryptowährungen setzen sich aus zwei Ebenen zusammen, der technischen Infrastruktur (genau hier finden wir die Blockchain) und der Anwendung für das Übertragen von Werteinheiten (Kryptowährung). Die Infrastruktur hat – insbesondere bei Bitcoin – seit Anfang 2009 unterbrechungsfrei ihren Dienst geleistet. Dies ist eine durchaus beachtliche Eigenschaft, denn normalerweise kann man sich eine Verfügbarkeit von de-facto 100 % nur mit äußerst kostspieliger technischer Ausstattung erkaufen (Cluster- und Failover-Lösungen für Datenbanken). Die hohe Verfügbarkeit bei niedrigen Kosten ist eine Eigenschaft, welche die Blockchain als Infrastruktur für eine Vielzahl von Prozessen interessant macht.

## **Missverständnis Nr. 4: „Die Blockchain ist sicher“**

Es kursiert die Auffassung, dass die Blockchain „sicherer“ ist als alles andere bisher Dagewesene. Der Begriff *Sicherheit* ist im Deutschen recht vielschichtig und fasst zusammen, was man im Englischen in „secure“ und „safe“ unterteilt. Mit „secure“ bezieht man sich auf die Resistenz gegen Cyber-Angriffe unterschiedlichster Art, also Man-in-the-Middle-Attacken, Penetrationsversuche, DoS-Attacken, Identitätsdiebstahl, etc. In die Kategorie „Safe“ fallen

## ■ Hype oder Hoffnung?

hingegen Eigenschaften wie sicher, robust oder verfügbar. In dieser Disziplin können Blockchains durchaus punkten.

Sie sollten aber auch im Bereich der „Security“ zumindest ein Sicherheitsniveau bieten, das auch bei klassischen verteilten Infrastrukturen zu finden ist, also typische IT-Sicherheitsanforderungen wie Verschlüsselung, Authentifizierung, Integrität und Nichtabstreitbarkeit sind Blockchain-unabhängig und auf technischer Ebene bei jeder Entwicklung verteilter Softwareanwendungen Grundvoraussetzung. Nicht jede Blockchain-Technologie unterstützt allerdings diese Sicherheitsmechanismen von Hause aus. Sie kann daher sogar sehr unsicher sein.

Es ist aber tatsächlich der Fall, dass die Blockchain einen neuen Sicherheitslevel hinzufügen kann. Ein klassisches, zentralisiertes System ist einem Angreifer hoffnungslos ausgeliefert, wenn dieser die Sicherheitshürden und Firewalls seiner IT-Infrastruktur überwunden hat. Dann kann der Angreifer tun und lassen, was er will: Daten löschen oder manipulieren, Anwendungen und Betriebssysteme mit eigenem Code infizieren, Bots installieren etc. Wenn nun aber eine Applikation Teil einer Blockchain ist, und diese im Rahmen eines Konsens gemeinsam mit anderen über die Datenwahrheit entscheidet, dann müsste der Angreifer einen großen Teil der Blockchain-Knoten überwältigen – und dies auch noch in kurzer Zeit, denn Anomalien lassen sich erkennen, so dass rechtzeitig Gegenmaßnahmen eingeleitet werden können.

Das entscheidende neue Sicherheitsmerkmal ist der Konsens über die Datenwahrheit über Organisationsgrenzen hinweg, und eine damit erhöhte Robustheit gegen Angriffe auf einzelne Knoten der Blockchain (siehe auch Kapitel 3.1 bzw. 3.3). Das heißt beispielsweise, dass es einem Angreifer erheblich schwerer fällt, bei der Lufthansa, British Airways, Delta, Iberia, Emirates und Air France gleichzeitig einzudringen, um damit eine Blockchain zu Fall zu bringen, die den Überfall auf bis zu 5 ihrer Mitglieder verkraften kann. Ausschließlich *in diesem Sinne* sind Daten in der Blockchain tatsächlich sicherer – aber immerhin!

### Missverständnis Nr. 5: „Datenschutz durch die Blockchain“

Erstaunlicherweise liest man häufig, dass die Daten in der Blockchain sicher sind – und dies sei daher gut für den Datenschutz.<sup>5</sup> Wie gesagt, was „sicher“ bedeuten kann, habe ich oben erörtert. Es muss sehr deutlich betont werden, dass Daten in der Blockchain grundsätzlich *transparent* sind – also ungeschützt! Das heißt, sie sind für jeden einsehbar, der auf die Blockchain zugreifen kann. „Grundsätzlich“ heißt, dass dies durch Verschlüsselungs- oder Verschleierungsmechanismen auf höherer Ebene abgeschwächt werden kann. Dann gelangt man jedoch häufig in schwierigeres Fahrwasser, was den Einsatz der Blockchain-Technologie grundsätzlich betrifft, denn mit verschlüsselten Daten kann ein Validator wenig anfangen.

---

5 Siehe z.B.: <http://versicherungswirtschaft-heute.de/maerkte-vertrieb/blockchain-der-assekuranz-ein-echter-innovationstreiber>

Zudem erfordert die Datenschutzgesetzgebung – zumindest mit der DSGVO in EU-Europa – dass eine Privatperson ein Recht auf Löschung von Daten hat, wenn diese nicht mehr für den ursprünglichen Zweck der Speicherung erforderlich sind. Dies verstößt natürlich gegen das hohe Gut der „Immutabilität“ einer Blockchain. Wenn man Daten aus der Historie wieder löschen kann, handelt es sich dann noch eine Blockchain? Ist denn das Prinzip „Blockchain“ überhaupt mit der Datenschutzgesetzgebung vereinbar? Blockchain und Datenschutz zu vereinen, ist offensichtlich ein schwieriges Unterfangen, siehe hierzu auch Kapitel 3.4.

### **Missverständnis Nr. 6: „Blockchain ist eine Datenbank“**

Unter einer „Datenbank“ würde man heute landläufig ein System verstehen, das über eine Anfrageschnittstelle und Indexierungsverfahren Daten inhaltsadressiert sehr effizient abrufbar macht und deren Konsistenz aufrechterhält. Praktisch erfolgt dies insbesondere durch ein relationales Datenmodell, bei dem der Zugriff durch SQL oder ähnliche Abfragesprachen möglich ist. All dies leistet eine Blockchain genau nicht! Jedenfalls in den meisten Fällen nicht. Es ist nicht die Hauptaufgabe einer Blockchain, Daten *effizient* zu verwalten. Die Blockchain ist eher eine Log-Datei, die durchaus in den Terabyte-Bereich wachsen kann. Eine solche Datei lässt sich jedoch nur linear durchscannen.

Wenn im Zusammenhang mit „Blockchain“ Datenbanken ins Spiel kommen, dann zumeist als Sekundärspeicher bzw. „Cache“, um es eben Anwendungen zu ermöglichen, effizient auf den Inhalt der Blockchain zuzugreifen.

Praktisch bedeutet dies, dass ein Blockchain-Projekt häufig ein separates Datenbank-Projekt nach sich zieht. Beteiligte wundern sich dann, dass diese eigentlich doch schlanke und effiziente Technologie in ihrer Anwendung plötzlich genau so aufwändig ist wie ein klassisches Projekt zur Anwendungsentwicklung. Verbleibender Zweck der Blockchain ist dann häufig nur noch, die Urkopie („Golden Copy“) einer Information zu beherbergen, auf die eher selten zugegriffen werden muss, beispielsweise zu Beweis Zwecken oder um die nächsthöhere Cache-Datenbank mit der „Wahrheit“ zu synchronisieren.

### **Missverständnis Nr. 7: „Aus dem Energieverbrauch des Mining definiert sich der Wert von Bitcoin“**

Eine interessante Aussage: „Mit dem Mining verbraucht man in hohem Maße Energie und hat dadurch erhebliche Kosten. Diese Kosten definieren dann den Wert der Bitcoins, die ein erfolgreicher Miner als Lohn erhält. Somit erhält die Währung „Bitcoin“ schließlich einen intrinsischen Wert. Dies ist fast eine marxistische These, der zufolge sich aus der geleisteten Arbeit der Wert des volkswirtschaftlichen Outputs definiert.

Sie ist jedoch falsch. Eine Kryptowährung und das Mining ihrer Werteinheiten sind zwei separate Märkte, die allerdings eng gekoppelt sind. Bitcoins an sich haben einen Preis, der

## ■ Hype oder Hoffnung?

sich wie bei jedem Gut aus der Nachfrage nach der Währung und dem verfügbaren Angebot ergibt – zu welchem Zweck auch immer. Will ich z.B. eine Pressemitteilung über Coin-Telegraph herausgeben, muss ich mir Bitcoins beschaffen, um sie zu bezahlen. Der Volkswirt nennt dies „Transaktionskassenhaltung“. Bin ich der Meinung, dass der Kurs von Bitcoin auf 100.000 Euro steigt, dann beschaffe ich mir Bitcoins als Wertspeicher bzw. als Anlagewährung. Es erfordert immer eine Community, die dem Gut „Kryptowährung“ einen Wert beimisst. Ansonsten könnte ja umgekehrt das Mining für eine Altcoin-Währung „Schwierig-Coin“ besonders aufwändig gestaltet werden, damit über möglichst viel Mining-Aufwand möglichst viel Wert in die Währung hineingetragen wird.

Es ist umgekehrt der Fall. Mining ist ein Geschäft. Ein Miner überprüft jeden Tag,

- wieviel ihn der Strom kostet,
- wie leistungsfähig seine Rechner sind,
- wieviel Belohnung ihm für das Mining aktuell winkt,
- in welcher Höhe er Transaktionsgebühren für sich verbuchen kann,
- und wie der Bitcoin-Kurs in Relation zu seinen Kosten steht.

Wenn diese Rechnung für ihn individuell aufgeht und er sich eine Erfolgswahrscheinlichkeit verspricht, bei dem ihm das Mining mehr einbringen wird als es ihn kostet, dann wird er minen – sonst nicht. Man kann dies anhand der weltweiten Hash-Power verfolgen, die sich mit der Kursentwicklung einer Kryptowährung aufbläht oder kontrahiert. Im Internet werden Statistiken geführt, die auf Basis von Bitcoin-Kurs, Stromkosten, technologischem Fortschritt und Preis von Mining-Hardware etc. anzeigen, ob es sich aktuell rechnet, in das Mining zu investieren. Näheres hierzu in Kapitel 3.

## Missverständnis Nr. 8: „Die Blockchain ist ein dezentraler Prozess“

Dies stimmt im Sinne der physischen Verteilung der Knoten einer Blockchain und auch im Sinne der replizierten Datenspeicherung, aber der Konsens als wichtiger Prozess beim Betrieb einer Blockchain besitzt zentralisierte Elemente, da immer genau ein Knoten für die Bildung eines neuen Blocks erforderlich ist. Dies führt zu schwerwiegenden Skalierungsnachteilen, die von Blockchain-Begeisterten nicht immer gerne zugegeben werden. Das Problem ist jedoch solange Blockchain-inhärent, wie von ihr erwartet wird, dass ein konsistenter Gesamtzustand erhalten bleibt.

So versuchen die Entwickler seit einiger Zeit, öffentliche Blockchains zu hierarchisieren (siehe z.B. „Polkadot“ in Kapitel 3.4), den Konsens auf weniger Knoten zu reduzieren (siehe „Proof of Authority“ in Kapitel 3.4) oder durch „Sharding“ den Datenbestand der Blockchain in ihre Teile zu zerlegen. Es wird dabei jedoch nur die Grenze der Skalierung unter Inkaufnahme hoher Komplexität verschoben.

Für eine Technologie, die ein logisch zentralisiertes Kassenbuch (engl. „Ledger“) pflegt, ist der Begriff „Distributed Ledger“ eher verwirrend: das Kassenbuch ist nicht verteilt in dem

Sinne, dass es verteilte Abschnitte davon gibt, es wird hingegen als genau ein logisch zentralisiertes Kassenbuch von verteilten Knoten gepflegt.

Wenn also der Anbieter einer Blockchain behauptet, dass sein System sowohl über Millionen Teilnehmer skaliert, zehntausende Transaktionen pro Sekunde verarbeiten kann und dies auch noch öffentlich, dann sollten auf absehbare Zeit alle Alarmlichter grell leuchten.

Andererseits gibt es interessante Entwicklungen, die zwar noch recht unerprobt sind, aber versprechen, Massentransaktionen öffentlich bei hohem Durchsatz zu bewältigen. IOTA und Hashgraph sind Beispiele hierfür. Leider sieht IOTA keine Blöcke vor und auch keine „Chain“. Aber hey! Solange Eigenschaften und Ziele einer solchen „Blockchain“ die gleichen bleiben, nehmen wir diese Technologie doch gerne in den Reigen der Blockchains auf. Siehe Kapitel 3.3.

### **Missverständnis Nr. 9: „Blockchain X verarbeitet 100.000 Transaktionen pro Sekunde“**

Super! Eine Blockchain, die 25.000 Transaktionen pro Sekunde schafft! Und dann kommt der Marketing-Mensch einer weiteren Technologie mit 100.000 Transaktionen pro Sekunde, und in der Podiumsdiskussion überbieten sich die Anbieter immer wieder neuer Technologien mit immer höher getriebenen Werten. Kürzlich meinte ein Ethereum-Fundamentalist wörtlich: „Ethereum is the fastest blockchain“. Nein. Ist sie nicht. Jedenfalls nicht mit den 10–20 Transaktionen pro Sekunde, die sie heute schafft. Auf Nachfrage kam dann die Korrektur: „Ethereum ist the fastest blockchain in the future“. Okay, wir werden es bezeugen dürfen ...

Aber nehmen wir einmal an, eine Blockchain schafft immerhin 10.000 Transaktionen pro Sekunde. Ist dies einmalig oder dauerhaft? Wieviele Knoten sind beteiligt? Und wie nahe stehen diese beieinander? Sind es evtl. nur einer oder zwei Knoten direkt auf den physischen Cores desselben Prozessors? Und wieviel Aufwand verursacht die Validierung pro Transaktion? Das kann oder will dann niemand genauer erklären. Und angenommen, es wären 10.000 Transaktionen mal 31,536 Mio. Sekunden im Jahr mal 100 Bytes pro Transaktion, dann wären dies stattliche 31,536 Terabytes. Ein ernstzunehmender Wert, insbesondere wenn davon nichts gelöscht werden darf (Immutabilität) und die gesamte Historie beim Hinzufügen eines Knotens erneut durchvalidiert werden muss. Man beachte: bei 170 GB Blockchain-Größe dauert dies bei Bitcoin bereits Tage.

Ich persönlich bin der Meinung, dass eine Blockchain-Technologie, die *auf Anwendungsebene* zuverlässig und dauerhaft 50 bis 100 Transaktionen pro Sekunde schafft, für den größten Teil aller B2B-Projekte ausreicht. Auch auf die Gefahr hin, in 50 Jahren als zweitgrößter Fehleinschätzer der Computergeschichte zitiert zu werden<sup>6</sup>. Vermutlich sind es nur einige hundert Prozesse weltweit, bei denen mehr als 50 bis 100 Transaktionen pro Sekunde verarbeitet werden müssen.

---

6 Der größte Fehleinschätzer war Thomas Watson, IBM-Vorstand im Jahr 1943, der damals prognostizierte: „Ich denke, dass es einen Weltmarkt für vielleicht fünf Computer gibt“.