Katarina Adam

# Blockchain-Technologie für Unternehmensprozesse

## Sinnvolle Anwendung der neuen Technologie in Unternehmen

Springer Gabler

# Blockchain-Technologie für Unternehmensprozesse

Katarina Adam

# Blockchain-Technologie für Unternehmensprozesse

## Sinnvolle Anwendung der neuen Technologie in Unternehmen

Springer Gabler

Katarina Adam
Hochschule für Technik und Wirtschaft
Berlin, Deutschland

ISBN 978-3-662-60718-3 ISBN 978-3-662-60719-0 (eBook)
https://doi.org/10.1007/978-3-662-60719-0

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

Springer Gabler


Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

*Für meine Tochter Marleen*

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| ABS | Asset-Backed Securities |
| ARPA | Advanced Research Projects Agency |
| BaFin | Bundesanstalt für Finanzdienstleistungsaufsicht |
| B2B | Business to Business |
| B2C | Business to Customer |
| BSI | Bundesamt für Sicherheits- und Informationstechnik |
| DDoS | Distributed Denial of Service |
| DLT | Distributed Ledger Technology (wird gern äquivalent zum Begriff Blockchain genutzt) |
| DNS | Domain Name System |
| EVM | Ethereum Virtual Machine |
| ggfs. | gegebenenfalls |
| GUI | Graphical User Interface |
| ff. | fortfolgende |
| ICO | Initial Coin Offering |
| IEO | Initial Exchange Offering |
| IFO | Initial Futures Offering |
| IPO | Initial Public Offering |
| IoT | Internet of Things |
| KAGB | Kapitalanlagegesetzbuch |
| KMU | klein- und mittelständische Unternehmen |
| KWG | Kreditwesengesetz |
| MAR | Marktmissbrauchsverordnung (Market Abuse Regulation) |
| MIFID II | Richtlinie über Märkte für Finanzinstrumente (Market in Financial Instruments Directive II) |
| PoA | Proof of Authority |
| PoB | Proof of Burn |
| PoET | Proof of Elapsed Time |
| PoI | Proof of Importance |
| PoR | Proof of Reputation |

| | |
|---|---|
| PoS | Proof of Stake |
| PoW | Proof of Work |
| P2P | Peer-to-Peer (vgl. Glossar unter Netzwerk) |
| SEC | Security and Exchange Commission |
| VAG | Versicherungsaufsichtsgesetz |
| VDI | Verband Deutscher Ingenieure |
| VermAnlG | Vermögensanlagengesetz |
| WpHG | Wertpapierhandelsgesetz |
| WpPG | Wertpapierprospektgesetz |
| ZAG | Zahlungsdiensteaufsichtsgesetz |
| ZKP | Zero Knowledge Proof |

# Einführung

1

**Zusammenfassung**

Dieses Buch dient dazu, Missverstände in Bezug auf diese Technologie aufzuklären, bestehende Ansätze zu erläutern und den/die Leser*in zu ermächtigen, für sich und den entsprechenden eigenen Anwendungsfall zu entscheiden, ob sich die Implementierung einer Blockchain-basierten Lösung lohnt. Dazu werden Begrifflichkeiten erläutert und im richtigen Kontext verortet.

Adressat dieses Buches sind klein- und mittelständische Unternehmen (KMU), die in Wertschöpfungsnetzwerken z. B. als Zulieferer agieren. Daneben soll es Interessierten, die sich eingehender mit den Anwendungsmöglichkeiten auseinandersetzen wollen oder müssen, helfen, sich strukturiert in die Materie einzudenken und einzuarbeiten.

Neben der Vermittlung des notwendigen Wissens um diese Technologie wird der Leser aufgefordert, sich mit seinen eigenen Prozessen auseinanderzusetzen. Nur wenn man seine eigenen Prozessstrukturen kennt, kann man Anforderungen ggf. an Dritte formulieren, diese Anforderungen technisch umzusetzen.

In den letzten Jahren gab es kaum ein Medium, das sich nicht mit dem Thema „Blockchain“ beschäftigt hat. Diese aufstrebende Technologie hat die Welt der Nerds und Early-Adapter verlassen und ist nun auf dem Weg, die Welt zu erobern. Hauptsächlich wird dies durch die auf die Blockchain-Technologie aufbauenden digitalen Währungen (Kryptowährungen)[1] wie z. B. Bitcoin, Etherium oder neuerdings auch durch Libra von Facebook und weitere erreicht.

[1] Kryptowährungen werden so genannt, weil Verschlüsselung und weitere kryptografische Elemente eine bedeutsame Rolle spielen, um zu vermeiden, dass das Geld mehrfach ausgegeben werden kann.



K. Adam, *Blockchain-Technologie für Unternehmensprozesse*,
https://doi.org/10.1007/978-3-662-60719-0_1

Die Enthusiasten behaupten daher auch, dass diese Technologie sich weiter auf alle anderen Industriezweige ausdehnen und die Welt quasi im Sturm erobern wird. Kritiker dagegen sehen diese Technologie lediglich als Nischentechnologie an, da sie den Beweis der Massentauglichkeit noch nicht erbracht hat. Um selbst eine Einschätzung und Bewertung vornehmen zu können, werden in diesem Kapitel die grundlegenden Konzepte der Technologie erläutert. Dazu wird beschrieben, welche verschiedenen Blockchain-Arten sich zu welchem Zweck (bisher) etabliert haben und welche technischen Konzepte hinter diesen Arten stehen.

„Geschichten von Revolutionen sind Geschichten des Unerwarteten, quasi des Unmöglichen, das dann doch geschieht", schreiben Patil und Moore in ihrem Buch „Entwertung".[2] Die Blockchain-Technologie wird gern als revolutionäre und disruptive Erweiterung des Internets beschrieben. Revolutionär deshalb, weil sie die klassischen Intermediäre, die wir heute in vielen Prozessen dazwischengeschaltet haben, überflüssig erscheinen lässt. Disruptives Potenzial ergibt sich aus dem Wegfall der Intermediäre, da nun ganz andere Geschäftsprozesse notwendig sind. Prozesse werden direkt (sogenannte Peer-to-Peer-Prozesse) und ohne Umwege über irgendwelche dazwischengeschalteten Positionen durchgeführt. Daher ist zu erwarten, dass diese Prozesse sich schlanker, effektiver, effizienter gestalten lassen und somit herkömmliche Ansätze überflüssig machen. Allein diese Aussicht muss jeden aufrütteln, weil das Bisherige überflüssig zu werden droht. Es ist wichtig, zu erkennen, welche Prozesse lohnenswert sind, um auf einer Blockchain dargestellt zu werden. Andere Prozesse hingegen müssen nicht neu gedacht werden, da sie, so wie sie aufgebaut und angelegt sind, den größtmöglichen Sinn stiften. Jedoch ermöglichen Blockchain-Lösungen, über den Tellerrand hinaus zu denken, sich also dem Unmöglichen zu nähern. Sie werden beim Lesen dieses Buches einige unerwartete Rückschlüsse ziehen können – ich hoffe, Sie haben beim Lesen und Entdecken neuer Möglichkeiten ebenso viel Freude, wie ich sie jeden Tag empfinde, wenn ich mich mit der Technologie und ihren Facetten beschäftige.

Eine wichtige Anmerkung zur Verwendung des Begriffs „Technologie" sei hier erwähnt:

Umgangssprachlich wird der Begriff „Technologie" sowohl als die „Lehre von der Technik" als auch „die vom Menschen erzeugten Gegenstände/Artefakte" synonym verwendet. Der Unterschied soll folgendermaßen beleuchtet werden:

▶ Der Verband Deutscher Ingenieure (VDI) spricht in seiner Richtlinie Nr. 3780 davon, dass unter Technik folgendes zu verstehen ist:

„Technik im Sinne dieser Richtlinie umfasst

- die Menge der nutzenorientierten, künstlichen, gegenständlichen Gebilde (Artefakte oder Sachsystem);
- die Menge menschlicher Handlungen und Einrichtungen, in denen Sachsysteme entstehen, und
- die Menge menschlicher Handlungen, in denen Sachsysteme verwendet werden.

[2] Patil, Raj; Moore, Jason W. (2018): Entwertung, S. 272.

Technikbewertung bezieht sich mithin nicht nur auf die gegenständlichen Sachsysteme, sondern auch auf die Bedingungen und die Folgen ihrer Entstehung und Verwendung.“[3]

Technik ist demnach entweder ein Gerät, ein Verfahren oder eine Fertigkeit und wird auch gern in Verbindung mit einem Handwerk verstanden.

Technologie ist hingegen die Lehre oder die Wissenschaft und setzt sich aus den beiden griechischen Wörtern „techne“ für Technik und „logos“ für Logik und/oder Vernunft zusammen und befasst sich mit den möglichen Methoden zur Erreichung eines definierten Ziels.[4] Neben der Anwendungsebene, die die technische Darstellung umfasst, gehören zur Technologie auch die übergeordnete Ebene der relevanten Umweltfaktoren und ihre Wechselwirkung auf die artifiziellen Sachsysteme.[5] Hierzu gehören wirtschaftliche, rechtliche, gesellschaftliche und soziale Faktoren, aus denen sich gemäß Hoffmann die „entscheidende Erweiterung des Technikbegriffes hin zur Technologie“ ableiten lässt.[6] Hoffmann verweist auf den Zielfindungsprozess, um mit vielschichtigen Problemstellungen aus unterschiedlichsten Quellen eine Lösung finden zu können, die über die reine anwendungsorientierte Technikebene hinausgeht.

Unterstützt wird dieses Verständnis zur Differenzierung zwischen Technik und Technologie durch den anwendungsorientierten Systemansatz von Bullinger, der darunter „[…] die Menge aller bekannten möglichen Methoden zur Erreichung eines Ziels in einem abgegrenzten Anwendungsbereich […] versteht“ (vgl. Abb. 1.1).[7]

Die Differenzierung der genutzten Begriffe ist insofern von Bedeutung, als mit diesen unterschiedlichen Begriffen auch unterschiedliche Ebenen angesteuert werden. So gilt es, den übergeordneten Rahmen der Blockchain-Technologie zu verstehen, um daran anschließend die Technik, das Anwenden zu beleuchten. Diese Differenzierung findet im angloamerikanischen Raum mit der Nutzung des Wortes „Technology“ nicht statt und kann beim simplen Übersetzen zu Missverständnissen führen.

Darum ist es wichtig, sich vorab zu verdeutlichen, welche Ebene angesprochen werden soll. Mehrheitlich wird es in diesem Buch um die Technik gehen, also um die Frage, wie und in welchem Kontext diese Technik für eine Geschäftsidee sinnvoll einsetzbar ist.

Werden diese Details und auch die sich eröffnende Komplexität nachvollzogen, dann wird der Technologie der Schleier des Hypes und/oder des Expertenwissens genommen. Je mehr Personen/Entscheider den Blick hinter die Kulissen wagen, je weniger lassen sie sich verführen und blenden von sagenhaften (und unrealistischen) Versprechen, die am Ende nur zu einer Enttäuschung führen. Aktionismus dieser Art war in den letzten zwei bis drei Jahren gut am Markt zu beobachten.

---

[3] VDI-Richtlinie 3780, S. 66.

[4] Duden: das Herkunftswörterbuch.

[5] Ropohl (1999), S. 117 ff: Sachsysteme werden als nutzenorientierte, künstliche gegenständliche Gebilde definiert und können als Oberbegriff für technische Hervorbringungen verstanden werden.

[6] Hoffmann (2011), S. 12.

[7] Bullinger (1994), S. 34.

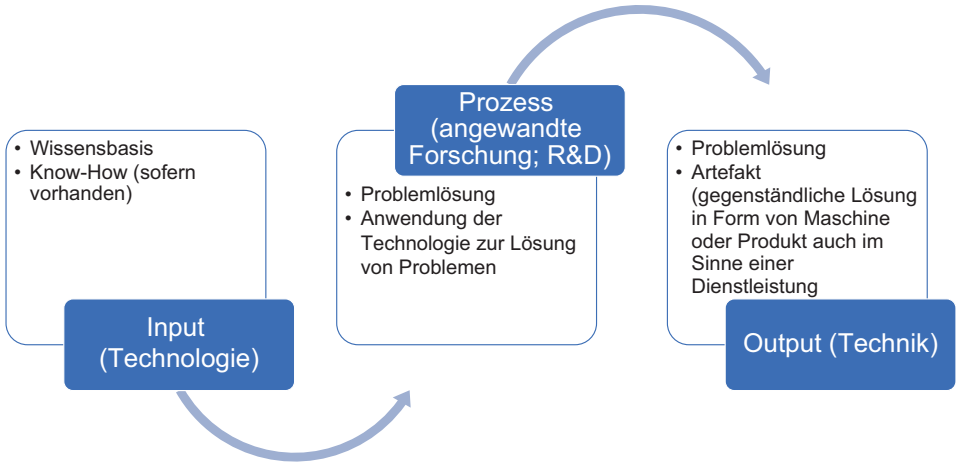


**Abb. 1.1** Technologie und Technik als anwendungsorientierter Ansatz nach Bullinger (eigene und ergänzte Darstellung)

Mein Anliegen mit diesem Buch ist, diese Technologie und Technik zu „entmystifizieren" und sie aus der Ecke des reinen Expertenwissens für die betriebswirtschaftlich denkenden Personen eines Unternehmens verständlich zu beschreiben. Es ist eine Gratwanderung zwischen den notwendigen Begrifflichkeiten mit technischen Details gepaart mit dem Übertrag in die betriebswirtschaftlichen Modelle und Denkweisen. Aus meiner Sicht ist dies notwendig, denn insbesondere in KMU ist das vorhandene Research-Budget zu gering und die bestehende IT-Abteilung zu sehr in die Tagesarbeit eingebunden. Hier muss die Geschäftsleitung voran gehen und das notwendige Wissen aufbauen, um strategische Entscheidungen treffen zu können. Die Entscheidung kann sich auch gegen den Einsatz dieser Technik und Technologie aussprechen – nur: Bevor diese Entscheidung getroffen wird, muss man wissen, was man ablehnt.

Lassen Sie uns daher starten!

## 1.1 Was ist „die" Blockchain-Technologie?

Zunächst, es gibt nicht „die" Blockchain, wohl aber die Lehre über die Blockchain. Damit ist der erweiterte Ansatz aus der Metaperspektive gemeint und gestattet die Betrachtung in Hinblick auf die Wechselwirkungen zwischen Umweltfaktoren (wirtschaftliche, rechtliche, gesellschaftliche und soziale Faktoren) und artifiziellen Sachsystemen (die verschiedenen Blockchain-Techniken, die Fragen nach „on-chain" und „off-chain"-Speicherungen[8] etc.).

[8] Unter „off-chain" versteht man Speichervorgänge, die nicht in der Blockchain, sondern in einer anderen Datenbank gespeichert werden.

Wenn auf eine Blockchain verwiesen wird, geschieht dies typischerweise im Rahmen von Kryptowährungen wie Bitcoin. Allerdings sind die Blockchain-Technologie und ihr Einsatzgebiet so viel größer, als dass sie „nur“ als Rückgrat der digitalen Währungen zum Einsatz zu kommen. Die Tech-Community und darüber hinaus viele weitere Teilnehmer sind sehr damit beschäftigt, andere innovative Wege zur Anwendung dieser Technologie zu finden. Prominentes Beispiel ist die Bankenindustrie.

Ganz pragmatisch kann man sich dieser Frage nähern, indem man sich die verschiedenen Arten und die damit einhergehenden Gestaltungsmöglichkeiten betrachtet (vgl. auch Abschn. 1.5), um die Wechselbeziehungen beschreiben zu können.

Die Blockchain-Technologie, und erweitert die sogenannte „Distributed Ledger Technology“ (DLT), basiert auf dezentralen Datenspeicher- und Verwaltungsfunktionalitäten.

▶ Eine Blockchain ist eine verteilte Datenbank, die eine Kette von digitalen Datenblöcken additiv speichert. Eine Blockchain kann auch als Distributed Ledger (verteilte Verzeichnisse) bezeichnet werden, jedoch muss nicht jedes verteilte Verzeichnis, das eine dezentrale Datenstruktur aufweist, eine Blockchain sein. Verteilte Verzeichnisse müssen jedoch nicht wie in einer Blockchain aneinandergekettet aufgebaut sein.

Liegt die verteilte Datenstruktur jedoch in Form einer Aneinanderkettung vor, bei der Transaktionen zu Blöcken zusammengefasst und mit sogenannten Hashes verkettet sind, dann handelt es sich um eine Blockchain.

Das Bundesamt für Sicherheit und Informationstechnik (BSI) hat diese Vielschichtigkeit in einer Grafik dargestellt (vgl. Abb. 1.2):[9]

Im Kern basiert die Technik auf einer Netzwerkstruktur sowie Konsensmechanismen innerhalb der Netzwerkstruktur (vgl. Kap. 2), Kryptografie (vgl. Abschn. 3.1), der Datenstruktur auf der Blockchain allgemein. In der Interaktion mit der den Kern umgebenden Infrastruktur stellen sich im Rahmen der Netzwerkstruktur die Fragen nach dem Netzwerkzugang an sich (vgl. Abschn. 1.5). Das ist eine so grundlegende Entscheidung, weil hiermit festgelegt wird, wer sich am Netzwerk beteiligen darf.

In diesem Zusammenhang der Teilnahme und Teilhabe müssen Antworten gefunden werden, über welche Schnittstellen die Teilnehmer eingebunden werden können. Zusätzlich muss bedacht werden, welchem Teilnehmer welche Rolle zugesprochen wird. Aus der Rolle heraus sind die Rechte und Pflichten abzuleiten. Unterstützt wird diese Anforderung durch kryptografische (Zusatz-)Funktionen.

Diese Abbildung verweist auf die (notwendige) Interaktion mit einer den Kern umgebenden Infrastruktur und macht gleichzeitig die Dimensionen sichtbar. Daher kann man in diesem Zusammenhang von der Blockchain-Technologie sprechen und zugleich auch eine Vorstellung über das große Potenzial dieser Technologie erhalten.

Um dieses Potenzial zu entfalten, müssen beide Ebenen (Kern und Infrastruktur) flexibel auf die an sie gestellten Anforderungen reagieren können. Die Blockchain-Technologie

[9] Berghoff et al. (2019), S. 11.

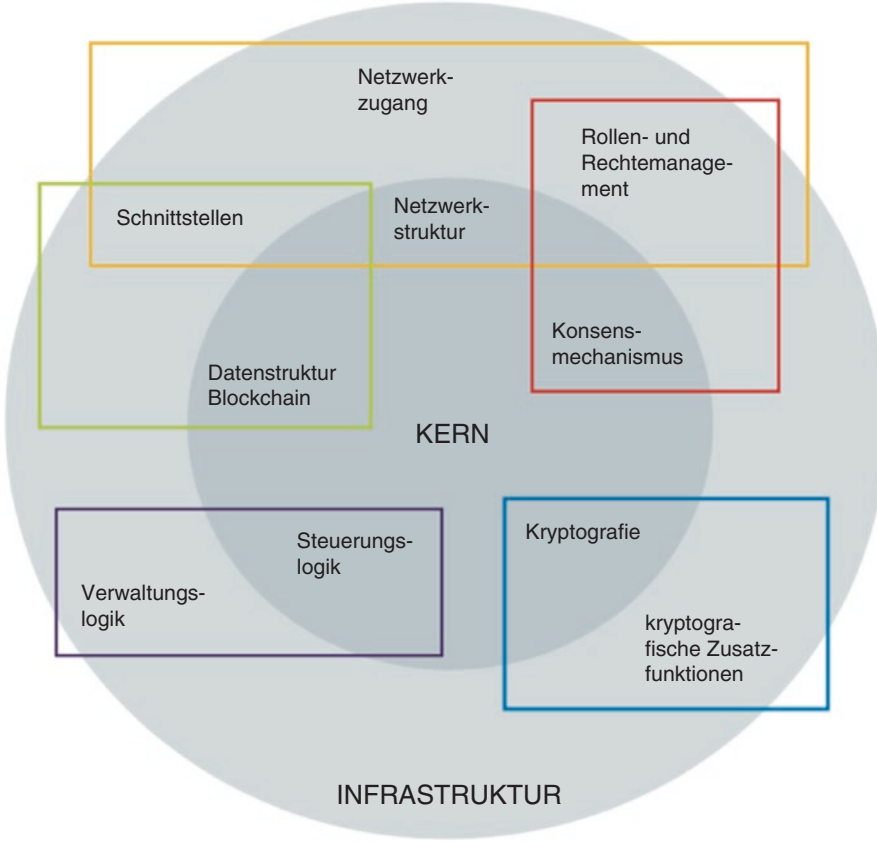


**Abb. 1.2** Blockchain-Schichtenmodell (Aus BSI 2019, Blockchain sicher gestalten; mit freundlicher Genehmigung von @BSI, All Rights Reserved)

als Ganzes muss sich weiterentwickeln. Ein kurzer Überblick zeigt auf, welche Phasen diese Technologie innerhalb der letzten Dekade seit Markteinführung durchlaufen hat.

So spricht man von der

- Blockchain-Technologie 1.0, wenn die Nutzung der Technik für reine Finanztransaktionen im Vordergrund stehen, so wie es von der Bitcoin-Anwendung geläufig ist.
- Blockchain-Technologie 2.0 befasst sich mit mehr als „nur" der Transaktion von Zahlungen. Mit der Erweiterung können Vermögensgestände (zumindest theoretisch) über sogenannte Smart Contracts (mehr dazu unter Abschn. 3.2) ohne jedweden Intermediär wie z. B. einen Notar zwischen zwei Teilnehmern transferiert werden.
- Blockchain-Technologie 3.0 befasst sich nicht nur mit den bisherigen Lösungskonzepten von den Vorgängern, sondern ist bestrebt, die Einschränkungen, die unter Blockchain 1.0 und 2.0 sichtbar sind, zu überwinden. Dazu gehört neben einer den Anforderungen der Wirtschaft angemessen Transaktionsrate auch die Fragen nach Energiekonsum, Blockgrößen und Skalierbarkeit.

Der Ausbau von dezentralen Datenspeichern in einer Netzwerkumgebung, in der das Netzwerk die Entscheidungen trifft, ist die grundlegende Basis dieser Technologie. Die Verwaltungsfunktionalitäten wirken nach innen, hinein in die Technik, sowie nach außen in die Infrastruktur. Diese Technologie ist am Werden, nicht am Sein. Dabei versteht sich diese Technologie als „open source", d. h. bestehende Urheberrechte gehören der Allgemeinheit, dem Netzwerk. Und damit arbeitet auch dieses Netzwerk (z. B. über GitHub) an der Weiterentwicklung dieser Technologie. Unbestritten ist jedoch auch, dass diese Technologie wirtschaftlich geprägte Geschäftsmodelle inspiriert und ermöglicht, um mit der Netzwerkstruktur innovative Produkte und Services zu entwickeln.

Zusätzlich, um die Terminologie mit einer weiteren Facette zu beleuchten, sei hier der Hinweis erlaubt, dass mit der fortschreitenden Digitalisierung (einhergehend mit der fortschreitenden Globalisierung) die sogenannte Plattformökonomie voranschreitet. Plattformen sind Netzwerke, siehe z. B. Amazon. Amazon bietet schon lange nicht mehr nur Bücher an, vielmehr kann der Kunde von A bis Z alles auf dieser Plattform kaufen. Unter Hinzuziehung externer Anbieter erhöht Amazon systematisch die Angebotspalette. Mittlerweile wird Amazon als Suchmaschine eingesetzt, d. h. Kunden, die etwas suchen, gehen bevorzugt über das Amazon-Portal ihrer Recherche nach.

Marketing-Experten erklären hierzu, dass wir alle zwar glauben zu wissen, wie viel Einfluss Amazon und andere digitale Unternehmen auf unseren Alltag haben, wir aber deren Macht noch immer systematisch unterschätzen.[10]

Und aus diesem Grunde ist die Bestimmung einer neuen Netzwerkorchestrierung notwendig. Blockchain-Technologie kann im übergeordneten Kontext dazu beitragen, dass die Marktmacht einzelner zugunsten eines verteilten Netzwerkes besser zu nutzen ist, und diese Technologie wird zur Erhöhung von Transparenz beitragen.

## 1.2 Was ist die Blockchain-Technik?

„Die" Blockchain-Technik beschreibt zunächst eine Datenbank, die jedoch verteilt auf den jeweils beteiligten Knotenpunkten bzw. Rechnern liegt und nicht zentral auf einem Rechner. Innerhalb dieser Datenbank werden Blöcke, gefüllt mit Daten, sicher aneinandergekettet. Diese Aneinanderkettung erfolgt strikt additiv, d. h. es wird immer ein Block an den vorherigen gehängt. Es ist nicht möglich, einen Block, eine Transaktion nachträglich in die bestehende Kette von Datenblöcken „hineinzuquetschen". Die Daten bzw. Transaktionen in so einem Block können Überweisungen, Bestellungen, Auftragserteilung, Bestätigungen der Echtheit oder sonstige Zertifikate und Ansprüche sein.

Ganz vereinfacht ausgedrückt kann man sich einen Block als Excel-Tabelle vorstellen, um die Idee nachvollziehen zu können. Im Fall von Kryptowährungen wie z. B. Bitcoin hat diese Excel-Tabelle drei systemnotwendige Spalten: „Nutzer A", „Nutzer B" sowie

[10] https://www.searchenginewatch.com/2019/08/01/amazon-google-market-share/, Steve Kraus: „Many people guess Amazon's market share at around 40–50 % – but that's how they perform in their worst categories, like clothing and furniture"; zugegriffen am 28.08.2019.

„Betrag“. Überweist nun Nutzer A dem Nutzer B eine bestimmte Summe an Kryptowährung, geschieht dies direkt, von Rechner zu Rechner.

In der Excel-Tabelle wird dieser Vorgang anonymisiert eingetragen, d. h. weder Nutzer A als Absender noch Nutzer B als Empfänger sind mit ihren Namen sichtbar. Zum eigentlichen Transfer einer digitalen Geldeinheit braucht man eine (in diesem Beispielfall) Bitcoin-Adresse als Public Key sowie einen Private Key. Die Bitcoin-Adresse kann durch einen Wallet-Anbieter generiert oder zufallsbasiert selbst erzeugt werden.[11] Öffentliche Schlüssel werden aus den privaten Schlüsseln mittels der elliptischen Kurve berechnet (vgl. Abschn. 3.1). Die Bitcoin-Adresse als Public Key wird gern mit einer E-Mail-Adresse verglichen, die jeder kennen darf. Das Postfach selbst kann aber nur derjenige öffnen, der das Passwort kennt. Bezogen auf dieses Beispiel entspricht das Passwort dem Private Key. Nutzer A verwendet somit den Private Key, um eine Transaktion über einen Betrag X an einen Empfänger zu signieren und ins Netzwerk zu senden. Das Netzwerk prüft, ob A über den zu sendenden Betrag verfügt, und bestätigt dann die Korrektheit der Transaktion, sofern das entsprechende Guthaben besitzt.

Wer eine neue E-Mail-Adresse erzeugt, muss sich immer auch ein Passwort überlegen. Ohne die Angabe des Passwortes wird keine neue E-Mail-Adresse generiert. Das Erzeugen der öffentlichen E-Mail-Adresse ist einfach, jedoch ist es mit heute existierender Rechen-Power nicht möglich, von dieser öffentlichen Adresse auf das private Passwort zurückzurechnen. Diese Eigenschaften macht sich auch die Blockchain-Technik zunutze.

Die Tabelle wird blockweise aktualisiert und liegt auf sämtlichen Rechnern des Netzwerkes. Das bedeutet, dass alle anderen Teilnehmer des Netzwerkes automatisch Buch über die getätigten Transaktionen führen und gleichzeitig bestätigen, dass diese Transaktionen tatsächlich stattgefunden haben. Die Saldostände sind öffentlich einsehbar.

Eigentümer von digitalen Währungen besitzen diese „nur“ in Form von Aufzeichnungen über Zu- und Abgänge. Es existieren weder physische noch digitale Einheiten von digitalen Währungen.

Derzeit werden viele Transaktionen papierbasiert oder teildigitalisiert abgewickelt. Unsere gesamte Wirtschaft ist noch immer auf Papierform an- und ausgelegt. So halten wir unsere Verträge ebenso auf Papier fest, wie wir per papierenem Stimmzettel wählen oder unsere Bankkonten verwalten. Ohne einen papierenen Beleg mangelt es an Vertrauen. Dies beruht z. T. auch darauf, dass Digitales einfach kopiert und vermehrt werden kann. Digitale Medien sind dynamisch im Gegensatz zu unserer bekannten statischen Papierwelt.

Nick Szabo stellt bereits 1997 fest, dass „digitale Medien Berechnungen durchführen, Maschinen direkt bedienen und einige Arten von Überlegungen viel effizienter durchführen können als Menschen“ (vgl. Szabo 1997 in Formalizing and Securing Relationships on Public Networks). Unser heutiges Vertrauen in die statische, weil papierbezogene Welt basiert darauf, dass die uns umgebenden Verträge und Gesetze von den Behörden/Institu-

[11] Bitadress.org zur zufallsbasierten Erstellung einer Bitcoin-Adresse und dem Erhalt des Private und Public Key, zugegriffen am 30.08.2019.

tionen interpretiert und durchgesetzt werden können. Doch dieser „Papierwahnsinn“ kostet viel Geld, ist fehleranfällig und sehr langsam.

Soll der Sprung in die Digitalisierung funktionieren, muss Vertrauen vorhanden sein, dass die digitale Welt für mindestens ebenso gute Absicherungen des Eigentums, der Vertragseinhaltung und -treue etc. bieten kann, wie wir es aus der analogen Welt kennen. Damit das gelingt, bedarf es der Nachvollziehbarkeit verbunden mit dem Wissen, dass keine so gesicherten Daten manipuliert werden können. Dieser Anspruch öffnet der Blockchain-Technologie die Türen, denn diese Technologie hat das Potenzial, die Lücke von der realen Welt in die digitale Welt zu schließen. Daten, die über eine Blockchain gespeichert werden, sind auf einer Vielzahl dezentral vernetzter Rechner gespeichert, die allesamt über dieselben komplexen Datenketten/Informationen verfügen. Der Versuch, einen einzigen Datenblock zu verändern oder gar zu löschen, wird aufgrund dieser Datenkettenstruktur fehlschlagen. Die Knotenpunkte/Rechner verfügen alle über dieselben Informationen und können sich daher auch gegenseitig kontrollieren. Ein veränderter Eintrag in einem Block führt zu einer falschen Kette. Da die anderen beteiligten Knotenpunkte diese Änderung nicht nachvollziehen können, den Wert somit nicht bestätigen können, bleibt diese neue Kette bedeutungslos – keine weitere Transaktion wird hier drangehängt, denn es fehlt die Validierung. Das System basiert auf der hinreichenden Bestätigung aller Beteiligten.

Blockchains können ihren Einsatz sowohl im Inter- als auch im Intranet finden. Ihre Faszination leitet sich aus der Vielseitigkeit ihrer Einsatzmöglichkeiten ab. Auch wenn Kritiker – zu recht – einwenden, dass der Massendurchbruch bisher noch nicht erfolgt ist, ist das Potenzial unbestritten. Den richtigen Anwendungsfall im eigenen Unternehmen zu bestimmen ist die Herausforderung.

Die Blockchain-Industrie kann schon jetzt modulartige Lösungen anbieten, die auf ihre Tauglichkeit zu bewerten dem Nutzer als Kunden obliegt. Am Ende aber muss jede Lösung einen Mehrwert aufweisen. Dazu ist ein erweitertes Wissen notwendig, um im richtigen Zusammenhang Entscheidungen treffen zu können.

### 1.2.1 Einsatz der Blockchain-Technik

Üblicherweise wird mit dem Einsatz dieser Technik die digitale Währung assoziiert. Wie aber bereits erläutert, ist Blockchain so viel mehr. Jedoch sind viele Projekte, die während des Höhepunkts des Hypes vorgestellt wurden, entweder völlig vom Markt verschwunden oder bestehen heute unter ganz anderen Voraussetzungen weiter fort. Was auch in der kommerziellen Softwareentwicklung sichtbar ist, nämlich dass Produkte ersonnen werden, die keinen Markt haben, ist auch für die Blockchain-Welt nicht anders. Die Blockchain als Technik einzusetzen, nur um eine Blockchain-basierte Lösung präsentieren zu können, ist nicht nachhaltig. Die Anforderungen, die eine immer komplexer und arbeitsteiliger werdende Welt bedingen, müssen dennoch erfasst und eingeordnet werden. Er-

schwerend kommt hinzu, dass die Technik über viele Facetten verfügt, die einen modularen Einsatz ermöglicht.

Dave Snowdon und Mary E. Boone entwickeln ein Framework (Snowden und Boone 2007), da sie feststellen, dass Führungskräfte trotz guter Ausbildung nicht immer in der Lage sind, die gewünschten Ergebnisse in Situationen zu liefern, die fast simultan eine Vielzahl an Entscheidungen fordern. Vielleicht ist bei der Frage, ob die Blockchain-Technologie in Ihrem Unternehmen Anwendung finden soll, nicht die zeitliche Komponente die entscheidende. Jedoch müssen sowohl die technischen, unternehmensorganisatorischen als auch die betriebswirtschaftlichen Aspekte bei der Fragestellung verstanden werden, und dies ist komplex. Daher lohnt sich die Betrachtung des Cynefin Framework nach Snowdon und Boone. Nach der kurzen Beschreibung der Domäneneigenschaften in diesem Modell wird dieses auf die Blockchain-Welt angewendet (vgl. Abb. 1.3).

Snowden und Boone haben fünf Domänen herauskristallisiert, die jeweils mit anderen Eigenschaften bestückt sind: einfach („simple“), chaotisch („chaotic“), kompliziert („complicated“), komplex („complex“) und Disorder im Sinne von „Nicht-Wissen, Regellosigkeit“.

Überträgt man diese Eigenschaften auf die Blockchain-Technologie und ihre Anwendungsmöglichkeiten, ergibt sich folgendes Bild:

### 1.2.2 Einfach (Best Practise)

Bei einfachen Problemen sind Ursache-Wirkung-Beziehungen offensichtlich und klar. Es gibt im Unternehmen existierende Lösungen, die quasi als Vorlage herangezogen werden können. Überführt man diesen Ansatz in die Blockchain-Umgebung, dann wird als Ergeb-

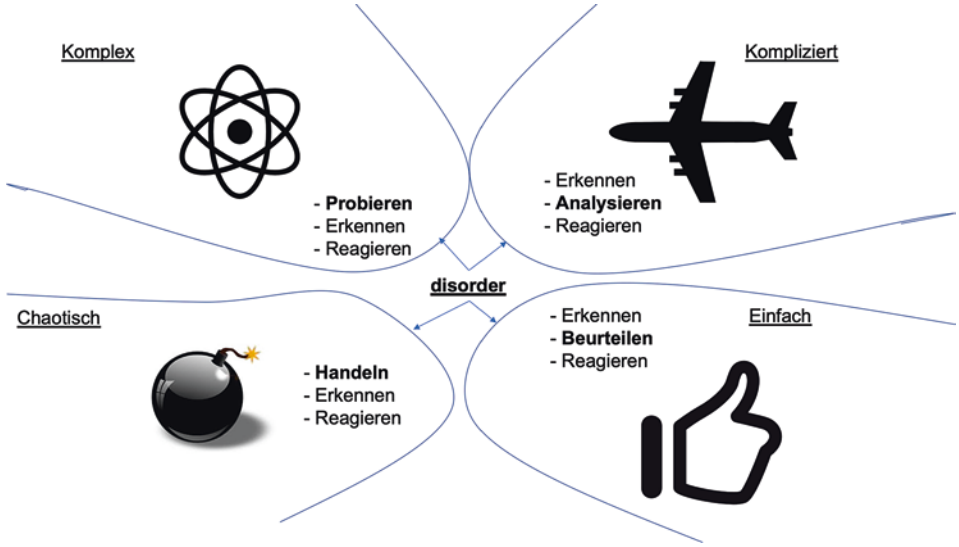


**Abb. 1.3** Cynefin Framework