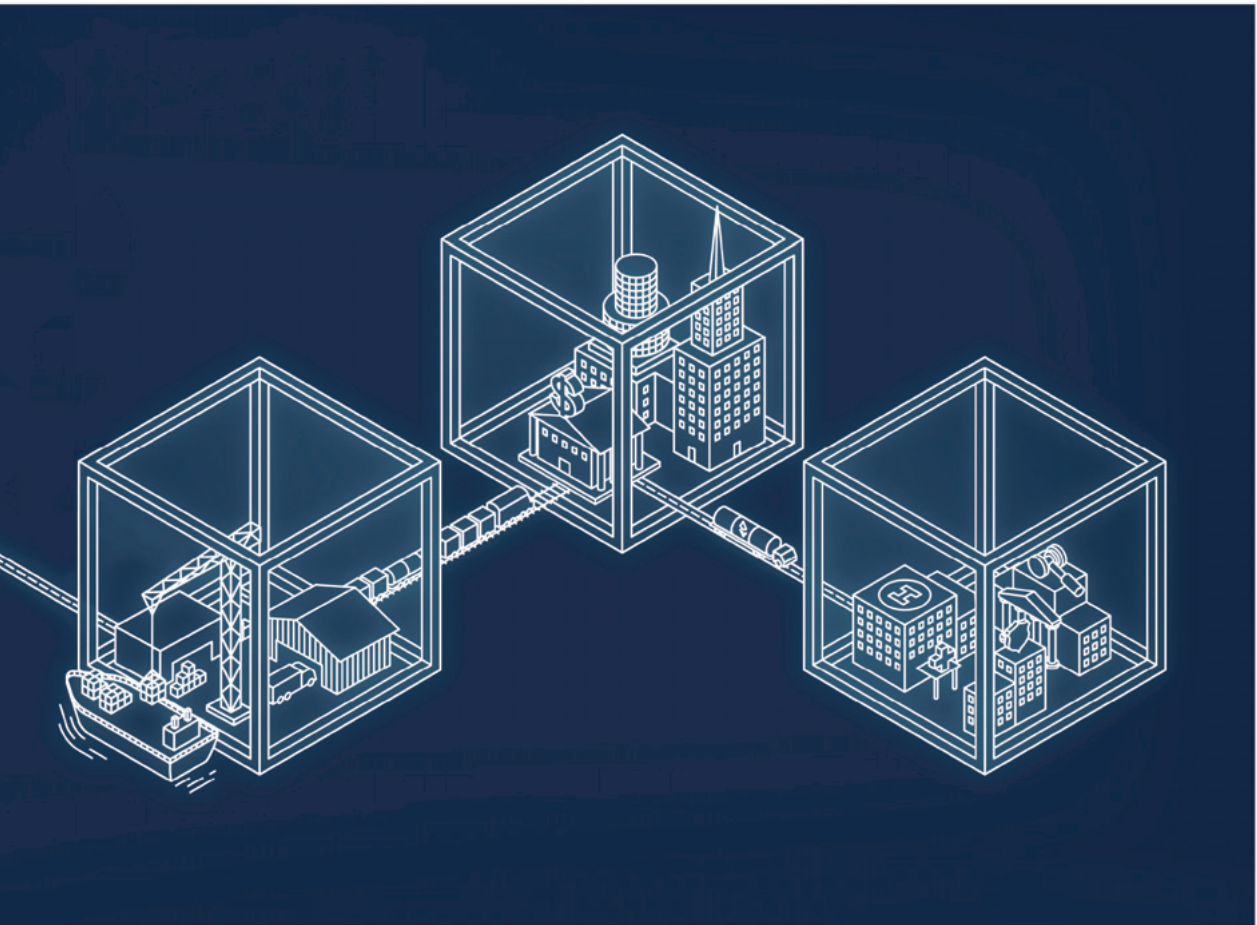


Pascal Egloff und Ernesto Turnes

Blockchain für die Praxis

Kryptowährungen, Smart Contracts, ICOs und Tokens



Pascal Egloff und Ernesto Turnes

Blockchain für die Praxis

Kryptowährungen, Smart Contracts, ICOs und Tokens

Die beiden Autoren haben zu gleichen Teilen das vorliegende Buch verfasst:



Ernesto Turnes ist seit 2006 vollamtlicher Professor für Finance an der FHS St. Gallen und leitet dort das Kompetenzzentrum Banking und Finance. Neben seiner Lehrtätigkeit im Bereich Aus- und Weiterbildung leitet er diverse Forschungs- und Dienstleistungsprojekte bei Banken und Vermögensverwaltern. Ernesto Turnes ist Co-Autor des Lehrbuches «Unternehmensbewertung und Aktienanalyse». Zu seinen Spezialgebieten zählen das Asset und Wealth Management sowie Blockchain und Krypto-Assets. Seit 2012 ist er Verwaltungsratspräsident eines Vermögensverwaltungsunternehmens mit Sitz in Lugano. Vor seiner Tätigkeit an der FHS St. Gallen arbeitete er als Aktienanalyst bei der Credit Suisse und als Kreditrisikomanager bei Raiffeisen Schweiz.

Ernesto Turnes hält zwei Master-Abschlüsse der Universität St. Gallen (HSG) in Banking und Finance sowie in Volkswirtschaftslehre. Zudem ist er CFA-Charterholder (Chartered Financial Analyst).



Pascal Egloff ist Dozent und Projektmanager an der FHS St. Gallen. Im Kompetenzzentrum für Banking und Finance leitet er Forschungs- und Dienstleistungsprojekte und unterrichtet im Rahmen von Aus- und Weiterbildungen. Zu seinen Spezialgebieten zählen Blockchain (für Unternehmen), Corporate Finance und Project Finance. Davor arbeitete er in London bei der Europäischen Bank für Wiederaufbau und Entwicklung (EBRD). Im Team für Power and Energy Utilities begleitete er Finanzierungsprojekte von erneuerbaren Energien im Raum Osteuropa und Zentralasien. Er verfügt zudem über fünf Jahre Berufserfahrung im Banking bei der Credit Suisse in der Schweiz sowie in London.

Pascal Egloff absolvierte einen Bachelor in Business Administration an der FHS St. Gallen und hält zwei Master-Abschlüsse der Universität St. Gallen (HSG) in internationalem Management (CEMS) sowie in Rechnungswesen und Finanzen (MAccFin). Zudem studierte er an der Aalto University – School of Business in Helsinki und ist zertifizierter Financial Risk Manager (FRM).

1. Auflage 2019

Pascal Egloff, Ernesto Turnes: Blockchain für die Praxis

ISBN 978-3-286-50305-2

Das Werk erscheint als E-Book unter der ISBN 978-3-286-11752-5 (PDF)

© Verlag SKV AG, Zürich
www.verlagskv.ch

Alle Rechte vorbehalten.

Ohne Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form zu reproduzieren.

Projektleitung und Lektorat: Silvester Popescu-Willigmann

Umschlagbild: Miloš Stojanović

Haben Sie Fragen, Anregungen oder Rückmeldungen?

Wir nehmen diese gerne per E-Mail an feedback@verlagskv.ch entgegen.

Vorwort

Digitalisierung ist *das* Schlagwort der Stunde. Egal ob Unternehmen, öffentliche Einrichtung oder Privatperson, alle gesellschaftlichen Gruppen haben Wissensbedarf und wollen bereit sein für die nächsten Entwicklungen im Bereich der digitalen Revolution. Innovationszyklen werden immer kürzer und zwingen Gesellschaft und Wirtschaft, ständig adaptionsfähig zu bleiben. Flexibel auf wechselnde Umweltbedingungen und Herausforderungen reagieren zu können, ist eine Grundvoraussetzung der heutigen Zeit.

Die Entwicklung der Blockchain-Technologie und deren Potenzial werden oft mit einem der Haupttreiber der Digitalisierung verglichen: dem Internet. Auch das Internet nahm am Anfang eine Nischenposition ein und entwickelte sich erst mit der Zeit zum gesellschaftsverändernden Phänomen. Nach dem ersten Hype wurde das World Wide Web zum Alltag und zur Selbstverständlichkeit. Die Internettechnologie ist zu einem Grundpfeiler für unternehmerischen Erfolg und wirtschaftliche Entwicklung geworden. Auch aus dem privaten Leben sind diese Technologien nicht mehr wegzudenken.

Die Blockchain-Technologie macht zurzeit eine vergleichbare Entwicklung durch. Immer mehr Menschen und Unternehmen befassen sich mit Praxis-Anwendungen und Weiterentwicklungen der Blockchain-Technologie. Obwohl Blockchain erst vor Kurzem Bekanntheit erlangt hat, wurde die Technologie an Grossanlässen wie dem World Economic Forum (WEF) bereits im Jahr 2015 thematisiert. Durch den Hype an den **Kryptomärkten** rückte das Thema auch in den Fokus eines breiteren Publikums. Blockchain wird jedoch oft und zu Unrecht auf den Bitcoin und andere Kryptowährungen reduziert. Die Blockchain-Technologie verfügt über weitaus vielfältigere Anwendungsfelder in der Praxis.

Wir sind davon überzeugt, dass Blockchain künftig einen **starken Einfluss** auf die Wirtschaft und die Gesellschaft haben wird. Wie und wann sich diese Technologie jedoch im grösseren Stil durchsetzen wird, kann nicht vorausgesagt werden. Die Blockchain wird oft auch als eine Art Katalysator für die Digitalisierung im weiteren Sinne verstanden. Mit diesem Buch beabsichtigen wir, den Leserinnen und Lesern die Blockchain-Technologie und ihre vielseitigen und branchenübergreifenden Anwendungsmöglichkeiten aus der **Perspektive der Praxis** auf verständliche Weise zu vermitteln.

Obschon sich das **Potenzial der Blockchain** in den letzten Jahren immer mehr offenbart hat, existiert im deutschsprachigen Raum kaum Literatur, welche die grundlegenden Strukturen und Zusammenhänge nachvollziehbar aufzeigt. Das vorliegende Buch bezweckt, diese Lücke zu schliessen, wobei es sich auf das Wesentliche fokussiert und einen systematischen Überblick über die in der Praxis am meisten verbreiteten Strukturen und Konzepte verschafft. Klarheit, Einfachheit und Verständlichkeit stehen im Mittelpunkt.

Didaktische Aufbereitung des Buches

Das Buch umfasst insgesamt drei Teile oder Ebenen: Technologien, Protokolle und Applikationen. Anhand einer **Leitgrafik** können die Lesenden stets nachvollziehen, auf welcher Ebene die jeweiligen Themen anzusiedeln sind. Jedes Kapitel beginnt mit einer **Box «Ausblick»**, die darauf hinweist, welche Inhalte im jeweiligen Kapitel enthalten sind. Am Schluss des Kapitels folgt jeweils eine **Box «Rückblick und Zusammenfassung»**, die alle wesentlichen Aspekte nochmals auflistet. In der Marginalspalte (am Seitenrand) wird den Lesenden angezeigt, ob im Text eine wichtige **«Definition»** oder ein anschauliches **«Beispiel»** zu finden ist. Zudem sind im Text folgende drei Arten von **Boxen** mit entsprechenden **Symbolen** integriert:

- **«Praxis»** mit Tipps und Hinweisen für Praxisorientierte
- **«Technik»** mit technischen Details für Technikinteressierte
- **«Exkurs»** mit Hintergrundinformationen für Detailverliebte

Diese Boxen können je nach Interesse auch übersprungen werden, ohne den roten Faden zu verlieren. Am Ende des Buches befindet sich zudem ein **Glossar** mit zahlreichen, nützlichen Begriffsdefinitionen.

Dieses Buch richtet sich an:

- Mitarbeitende und Führungskräfte von Unternehmen und der öffentlichen Verwaltung, die das Potenzial und die Funktionsweise der Blockchain-Technologie besser verstehen möchten.
- Anlegerinnen und Anleger, die sich für Investments im Bereich der Kryptowährungen und Tokens interessieren.
- Studierende von Fachhochschulen und Universitäten sowie Teilnehmende von Weiterbildungslehrgängen.
- Blockchain-Interessierte, die sich mit dieser innovativen Technologie vertieft auseinandersetzen möchten.

Folgenden Personen, die zum Gelingen dieses Buches beigetragen haben, möchten wir einen **speziellen Dank** aussprechen:

- Der Fachbereichsleiterin Prof. Dr. Sibylle Minder Hochreutener und unserem Institutsleiter Prof. Dr. Roland Waibel, für die Unterstützung unseres Buchprojekts.
- Den Fachexperten Christoph Burgdorfer (Unternehmer und Blockchain-Experte aus London) und Thomas Müller (Partner bei Walder Wyss, Zürich), die uns wertvolle Inputs aus der Praxis gegeben haben.
- Allen Personen aus dem Verlag SKV, insbesondere Silvester Popescu-Willigmann und Kirsten Rotert, welche die professionelle Umsetzung und Publikation sicherstellten.

Um unserer Leserschaft zu ermöglichen, bei dieser dynamischen Thematik laufend auf dem **aktuellen Stand** zu bleiben, haben wir für unser Buch eine **eigene Webseite** erstellt (www.blockchain4u.ch). Wir bitten Sie, uns Ihre Kommentare und Verbesserungsvorschläge über diesen Kanal mitzuteilen.

Wir wünschen allen Leserinnen und Lesern viel Spass bei der Lektüre und hoffen, mit unserem Buch eine Inspirationsquelle für künftige Blockchain-Projekte zu sein.

St. Gallen, im November 2018

Ernesto Turnes und Pascal Egloff

Symbole für die im Buch verwendeten Boxen



= Praxis



= Technik



= Exkurs

Inhalt

Das Wichtigste in Kürze	12
1 Einleitung	15
1.1 Digitalisierung und Blockchain	15
1.2 Aufbau und Leitgrafik	16
1.3 Aktualität und Webseite	18
Teil I: Technologien	20
2 Einführung Technologie	21
2.1 Von zentralen zu verteilten Netzwerken	21
2.2 Transaktionssysteme	24
2.2.1 Aufgaben eines Transaktionssystems	24
2.2.2 Anforderungen an ein Transaktionssystem	25
2.2.3 Alternative Transaktionssysteme	27
2.3 Verteilte Transaktionssysteme (DLT)	27
2.4 Unterscheidung DLT – Blockchain	31
3 Blockchain	33
3.1 Einleitung	33
3.2 Verfügbarkeit	35
3.2.1 Verteiltes Peer-to-Peer-Netzwerk	36
3.2.2 Private versus öffentliche Blockchain	38
3.3 Eigentumssicherung	40
3.3.1 Einführung Kryptografie	40
3.3.2 Asymmetrische Kryptografie	42
3.3.3 Wallets zur Schlüsselaufbewahrung	44
3.4 Unveränderbarkeit	45
3.4.1 Bestandteile eines Blocks	46
3.4.2 Verkettung von Blöcken	47
3.4.3 Append-Only-Regel	50
3.5 Überprüfbarkeit	51
3.5.1 Von der Transaktion zum Block	52
3.5.2 Arbeitsnachweis (Proof of Work, Mining)	55

3.5.3	Beteiligungsnachweis (Proof of Stake, Forging)	61
3.5.4	Weitere Konsensmechanismen	64
3.6	Skalierbarkeit	64
3.6.1	Anzahl Transaktionen als Engpass	65
3.6.2	Transaktionskosten als regulierender Faktor	66
3.6.3	Transaktionen pro Block und Merkle Tree	67
4	DAG (Directed Acyclic Graph)	71
Teil II: Protokolle		76
5	Einführung Protokolle	77
5.1	Was ist ein Protokoll?	77
5.2	Protokollanpassungen (Soft und Hard Forks)	79
6	Kryptowährungen und Tokens	81
6.1	Kategorisierung	84
6.2	Handel	87
6.2.1	Wallets	87
6.2.2	Kryptobörsen	94
6.2.3	Finanzprodukte	97
6.3	Bitcoin	99
6.3.1	Entstehung und Kursentwicklung	99
6.3.2	Eigenschaften und Funktionsweise	103
6.3.3	Abspaltungen	111
6.3.4	Stärken und Schwächen	112
6.4	Ether (Ethereum)	116
6.4.1	Entstehung und Kursentwicklung	116
6.4.2	Eigenschaften und Funktionsweise	117
6.4.3	Abspaltungen	123
6.4.4	Stärken und Schwächen	125
6.5	MIOTA (IOTA)	128
6.5.1	Entstehung und Kursentwicklung	128
6.5.2	Eigenschaften und Funktionsweise	130
6.5.3	Stärken und Schwächen	132
6.6	Rechtliche, steuerliche und buchhalterische Aspekte	134
6.7	Zentralbank-Kryptowährungen	135

Teil III: Applikationen	138
7 Einführung Applikationen	139
7.1 Smart Contracts	141
7.1.1 Schnittstellen und Oracles	143
7.1.2 Rechtliche Sichtweise	146
7.1.3 Smart Contracts als Grundstein	147
7.2 Initial Coin Offering (ICO)	147
7.2.1 Statistische Daten	148
7.2.2 ERC20-Tokens	151
7.2.3 Analyse und Bewertung	153
7.2.4 Rechtliche Aspekte	154
7.3 Dezentrale Applikationen (DApps)	155
7.3.1 Abgrenzung	155
7.3.2 Wichtige Elemente	156
8 Blockchain für Unternehmen	159
8.1 Von der Nische zum Mainstream	159
8.2 Potenzialanalyse	161
8.2.1 «Blockchain-Instrumente» für Unternehmen	162
8.2.2 Bisherige Modell-Ansätze	162
8.2.3 Blockchain-Entscheidungs-Modell	163
8.2.4 Private Blockchains für Unternehmen	167
8.3 Ausblick und Use Cases	169
Glossar	173
Quellenverzeichnis	181
Bücher und Studien	181
White Papers	182
Online-Quellen	183

Das Wichtigste in Kürze

Um den **Einstieg** in die komplexe Welt von Blockchain und Kryptowährungen zu erleichtern und einen **gemeinsamen Startpunkt** zu schaffen, werden nachfolgend die wichtigsten Begrifflichkeiten und Konzepte anhand von **Fragen und Antworten** eingeführt und erläutert.

Was ist eine Blockchain?

Der Begriff «**Blockchain**» steht für eine Vielzahl an neuen Möglichkeiten, eine ganze Bewegung innerhalb der Digitalisierungswelle sowie eine Kombination von teils schon länger bestehenden Technologien. Allgemein ist unter einer Blockchain (Blockkette) eine **verteilte Transaktionsdatenbank** zu verstehen, die den sicheren **Transfer** und das Speichern von Daten, Werten und Programmen ermöglicht. Dieses verteilte Netzwerk besteht aus unzähligen Computern, die gemeinsam in einem **öffentlichen Register** alle Transaktionen zwischen den Teilnehmenden **sicher, nachvollziehbar und unveränderbar** festhalten. Diese **Dezentralität** stellt sicher, dass wenn ein oder mehrere Teilnehmende angegriffen werden, die Integrität des Gesamtsystems bestehen bleibt. Die technischen Eigenschaften der Blockchain tragen dazu bei, das notwendige Vertrauen für den Transfer von Vermögenswerten und Rechten auch ohne einen Mittelsmann (Intermediär) zu schaffen. In Zukunft könnten **zentrale Vertrauensinstanzen** wie beispielsweise Banken, Versicherungen und Börsen teilweise oder gar ganz ersetzt werden. In vielen Fällen handelt es sich bei den derzeitigen Einsatzgebieten in erster Linie um **Prozessoptimierungen** und nicht um eine vollständige Substitution eines Intermediärs.

Wie funktioniert die Blockchain?

Alle Transaktionen werden in **Blöcke** mit einer bestimmten Blockgrösse verpackt. Bevor die Blöcke in chronologischer Reihenfolge an die Blockchain angehängt werden, ist die **Gültigkeit der Transaktionen und Blöcke** zu überprüfen. Das Ziel dieser **Überprüfung** besteht darin, unter den unbekanntenen und verstreuten Netzwerk-Teilnehmenden einen **Konsens** über die Gültigkeit der Blockchain zu erlangen. Je nachdem, welches **Konsensverfahren** dafür vorgesehen ist, kann diese Überprüfung mit einem enormen **Rechenaufwand und Energieverbrauch** verbunden sein. Um zu verhindern, dass überprüfte Transaktionen nachträglich verändert oder manipuliert werden, enthält jeder Block Informationen über den vorherigen Block. Diese **Verkettung der Blöcke** ist für die **Unveränderbarkeit** der Blockchain verantwortlich. Diese Unveränderbarkeit sollte unter anderem zur Bildung von **Vertrauen** in die Blockchain und ihre Anwendungen beitragen.

Welche Rolle spielt die Kryptografie?

Durch die **Verschlüsselung von Transaktionen** (Kryptografie) wird sichergestellt, dass nur der beabsichtigte Empfänger die Transaktion wieder entschlüsseln kann. Ferner wird gewährleistet, dass der Sender nur Vermögenswerte und Rechte transferieren kann, die sich auch in seinem Besitz befinden. Alle Transaktionen, die auf der Blockchain erfasst werden, verfügen über einen Sender und einen Empfänger. Die Persönlichkeitsdaten der Teilnehmenden sind jedoch unbekannt. Diese Anonymität (genauer gesagt **Pseudonymität**) hat den Nachteil, dass sie unter Umständen für illegale Machenschaften missbraucht werden kann.

Was sind Kryptowährungen und Tokens?

Bei **Kryptowährungen und Tokens** handelt es sich im Gegensatz zur Blockchain nicht um Technologien, sondern um **Anwendungen** der Technologie. Der Begriff «Kryptowährungen» ist im Zusammenhang mit der virtuellen Währung Bitcoin entstanden, obschon der Bitcoin die **volkswirtschaftlichen Funktionen** einer Währung derzeit (noch) nicht erfüllt. In Fachkreisen wird daher anstelle von Kryptowährungen zunehmend von **Tokens (Wertmarken)** gesprochen. Es gibt derzeit über 2000 Tokens, die je nach Funktion in **Zahlungs-, Nutzungs- und Anlage-Tokens** unterteilt werden.

Wie können Kryptowährungen und Tokens gehandelt werden?

Kryptobörsen bieten die Möglichkeit, Kryptowährungen und Tokens zu kaufen und zu verkaufen. Bevor mit dem Handel von Kryptowährungen und Tokens losgelegt wird, ist eine **Registrierung** an einer Kryptobörse erforderlich. Weil es in der Vergangenheit immer wieder zu Hacker-Angriffen auf die **Exchange Wallets** an den Kryptobörsen gekommen ist, sollten die gekauften Kryptowährungen und Tokens nach dem Kauf auf ein eigenes, separates Wallet transferiert werden.

Was ist ein Smart Contract?

Smart Contracts («intelligente Verträge») erlauben es, die Vorteile von Blockchain für eine Vielzahl von **weiteren Anwendungsfeldern** als nur Kryptowährungen und Tokens zu nutzen. Einige Blockchains können neben der Abwicklung von Transaktionen auch Smart Contracts abspeichern und ausführen. Dabei handelt es sich um Programme, die automatisch ausgeführt werden, sobald gewisse Bedingungen erfüllt sind. In der Praxis werden laufend neue Anwendungsfelder für Smart Contracts entdeckt und erschlossen.

Was ist ein Initial Coin Offering (ICO)?

Bei ICOs handelt es sich um eine **Kapitalaufnahme**, die mit dem **Crowdfunding** vergleichbar ist. Das ICO dient meist der **Finanzierung eines Projekts** (z. B. Entwicklung

einer Technologie), das in einem sogenannten **White Paper** beschrieben ist. Alle Investierenden, die an ICOs partizipieren möchten, überweisen den jeweiligen Betrag an die Adresse eines **Smart Contracts**, der dann die **neuen Tokens automatisch** an die Adressen der Investierenden ausbezahlt. Insbesondere für **technologiebasierte Start-ups** sind ICOs eine interessante Möglichkeit zur Finanzierung eines Projektvorhabens. ICOs sind aber auch für Unternehmen ausserhalb der Technologiebranche durchaus interessant.

Welche Rolle spielt Blockchain bei Unternehmen?

Die Blockchain-Technologie darf nicht einfach auf Kryptowährungen und Tokens reduziert werden. Sie verfügt prinzipiell über **unzählige Anwendungsmöglichkeiten in allen Branchen**. Da sich diese Entwicklungen derzeit aber noch in den **Kinderschuh**en befinden, wird sich erst in Zukunft erweisen, **welche Anwendungen** sich durchsetzen werden. Für Unternehmen ist es deshalb umso wichtiger, die Entwicklung der Blockchain-Technologie aktiv mitzuverfolgen und erste Erfahrungen zu sammeln.

1 Einleitung

Ausblick Kapitel 1

In diesem Kapitel erfahren Sie,

- welche Verbindung zwischen der Digitalisierung und der Blockchain-Technologie besteht,
- wie vielfältig die Anwendungsbereiche von Blockchain sein können,
- wie das Buch und die Leitgrafik strukturiert sind und
- die drei Ebenen der Blockchain-Welt: Technologien, Protokolle und Applikationen.

1.1 Digitalisierung und Blockchain

Seit einigen Jahren schreitet die **Digitalisierung** unaufhaltsam voran und dringt bis in alle **wirtschaftlichen und gesellschaftlichen Bereiche** vor. Dabei handelt es sich nicht um eine vorübergehende Erscheinung, sondern vielmehr um einen **nachhaltigen Megatrend**. Der Begriff «Digitalisierung» bezeichnet die Umwandlung von analogen Informationen in eine **digitale Form** zum Zwecke der Speicherung, Verarbeitung und Nutzung durch elektronische Datenverarbeitungssysteme. Physische Objekte, Ereignisse oder analoge Medien werden in einen **binären Code**, bestehend aus den **Werten 0 oder 1**, übersetzt. Die **digitale Transformation** – teilweise wird auch von **digitaler Revolution** gesprochen – basiert somit auf einem technologischen Fundament. Der digitale Wandel und entsprechende, neue Technologien bergen vielfältige Chancen sowie Risiken und ermöglichen eine ganze Palette **neuer Geschäftsmodelle**.

Definition

Trotz **unzähliger Anwendungsfelder**, die durch die digitale Infrastruktur ermöglicht werden, steht im Mittelpunkt immer der Mensch. Die Technologien sollen das Leben vereinfachen und nicht dem Selbstzweck dienen. In Zukunft werden immer mehr Daten über unsere Arbeits- und Lebenswelt generiert und abgelegt. Zudem werden immer mehr **Dinge** (Geräte, Maschinen) mit **Sensoren** ausgestattet, die ihre Umwelt wahrnehmen und darauf reagieren können. Es zeichnet sich auch ab, dass immer mehr Dinge direkt mit anderen Dingen kommunizieren werden, im sogenannten «**Internet der Dinge**» (Internet of Things, IoT). Vor diesem Hintergrund werden **Cybersecurity** und der **sichere Umgang mit Daten** nicht nur heute, sondern auch in Zukunft eine grosse Herausforderung darstellen.

Kryptowährungen sind nur *ein* Anwendungsbereich

Definition

Im Kontext der Digitalisierung kann die Blockchain-Technologie eine wichtige Rolle spielen. Der Begriff «Blockchain» wird im Volksmund meist mit dem Bitcoin gleichgesetzt. **Kryptowährungen und Tokens** sind jedoch nur *ein* Anwendungsbereich der Blockchain-Technologie. Die Blockchain beschreibt vielmehr eine umfassende, **grundlegende Technologie**. Diese besteht aus mehreren Bestandteilen oder **Teiltechnologien**, die zusammen ein Konstrukt bilden, das «Blockchain» genannt wird. Die Blockchain-Technologie kann in beliebigen Bereichen angewendet werden, um **Prozesse zu vereinfachen** oder **neue Geschäftsmodelle** zu ermöglichen. Zudem steht «Blockchain» für eine gesamte Bewegung von **dezentralen oder verteilten Transaktionssystemen**.

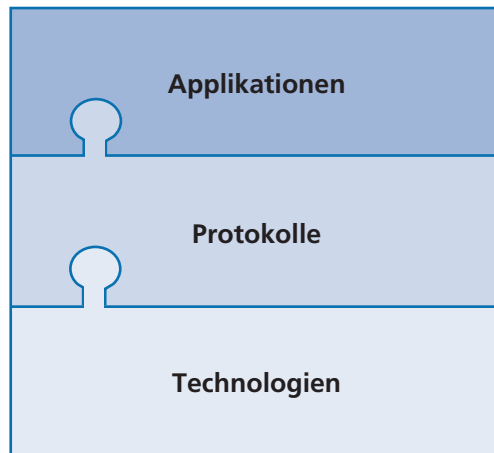
Weitere Anwendungsbereiche von Blockchain

Die Anwendungsmöglichkeiten der Blockchain-Technologie sind sehr vielfältig. Die Technologie besitzt das Potenzial, in fast allen Branchen und Bereichen von Wirtschaft und Gesellschaft Optimierungen und neue Kollaborationsmodelle zu ermöglichen. Anwendungen wie **Smart Contracts**, **Initial Coin Offerings (ICOs)** und **dezentrale Applikationen (DApps)** gehören ebenfalls zum Themenfeld rund um die Blockchain. All diese Begriffe hängen zusammen und müssen im gemeinsamen Kontext betrachtet werden. Wenn man sich erstmals mit Blockchain beschäftigt, kann dies durchaus für Verwirrung sorgen. Die isolierte Beantwortung einer Frage führt oft zu weiteren Fragen. Zudem ist das Wissen über Blockchain derzeit sehr fragmentiert oder meist nur in «unpassender Flughöhe» verfügbar. Das vorliegende Buch soll genau an diesem Punkt ansetzen. «Blockchain für die Praxis» bietet einen strukturierten Aufbau, der die verschiedenen Teilkonzepte verknüpft und die Thematik **ganzheitlich und praxisnah** beleuchtet. Die Erfahrung in der Praxis zeigt, dass im Rahmen von Potenzialabklärungen für Blockchain oft auch neue Ideen für Digitalisierungsprojekte entstehen.

1.2 Aufbau und Leitgrafik

Dieses Buch funktioniert ähnlich wie ein **Kochbuch**. Einerseits werden **Grundlagen und Strukturen** eingeführt und andererseits werden «Rezepte» für die **praxisnahe Umsetzung** angeboten.

Der Aufbau dieses Buches basiert auf drei Teilen oder Ebenen: Der erste Teil befasst sich mit den **Technologien**, der zweite Teil mit den **Protokollen** und der dritte Teil mit den **Applikationen**.



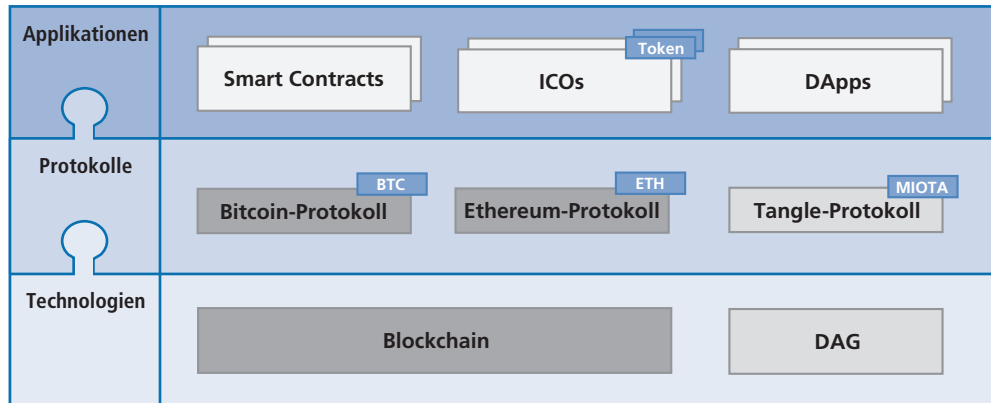
In der **Leitgrafik** auf der folgenden Seite werden diese drei Ebenen noch weiter verfeinert. Auf der ersten Ebene befinden sich die **Technologien**. Sie bilden das **Fundament** für die Protokolle und die Applikationen. Die Blockchain-Technologie stellt nur *eine* mögliche Variante von **verteilten Transaktionssystemen (Distributed Ledger Technology, DLT)** dar. Weitere Technologien wie zum Beispiel DAG (Directed Acyclic Graph) zählen ebenfalls zu den DLT-Systemen.

Auf der zweiten Ebene unserer Leitgrafik befinden sich die **Protokolle**. Sie bestimmen die Ausgestaltung der Blockchain-Technologie und können auch eine **Plattformfunktion** beinhalten. Diese Plattform kann als Basis für diverse **Applikationen** (dritte Ebene in der Leitgrafik) dienen.

Das folgende Beispiel aus dem Alltag soll zum besseren Verständnis beitragen: Es gibt **Beispiel** viele verschiedene **Arten von Milch** (in unserem Fall verteilte Transaktionssysteme). Wir beschäftigen uns nun insbesondere mit **Kuhmilch** (d. h. eine der **Technologien** unter dem Überbegriff DLT, in unserem Fall Blockchain). Mit der Kuhmilch stellt eine Molkerei **Butter** her (in unserem Fall entspricht die Butter einem **Protokoll**). Butter kann man einerseits eigenständig als Nahrungsmittel verwenden oder man kann sie nutzen, um einen **Kuchen oder Kekse** zu backen (diese Produkte entsprechen in unserem Fall den **Applikationen**). Um einen genießbaren Kuchen zu backen, benötigen wir die passenden Produkte (Butter und nicht Milch). Im Beispiel von Milch, Butter und Kuchen ist es stets klar, von **welchem Prozessschritt** wir gerade sprechen. Bei Blockchain, Kryptowährungen und Co. ist die Unterscheidung der drei Ebenen jedoch nicht immer eindeutig.

«**Blockchain für die Praxis**» gibt klare Strukturen vor, die dabei unterstützen, die diversen Bausteine rund um das Themenfeld «Blockchain» richtig einzuordnen. Die fol-

gende Leitgrafik erweitert die drei Ebenen um wichtige Begrifflichkeiten und konkrete Beispiele. Es handelt sich dabei nicht um eine abschliessende Aufzählung.¹ Unsere **Leitgrafik** wird uns durch das ganze Buch begleiten und als Orientierungshilfe dienen. Alle Begriffe werden im Verlauf dieses Buches erläutert.



1.3 Aktualität und Webseite

Das ganze Themenfeld rund um Blockchain, Kryptowährungen und Co. entwickelt sich **sehr dynamisch**. Durch den steigenden Ressourceneinsatz seitens grosser Akteure² werden die **Innovationszyklen** immer kürzer. Obwohl «Blockchain für die Praxis» hauptsächlich Grundlagenstrukturen und -konzepte vermittelt, ist das Buch ebenfalls der Marktdynamik ausgesetzt. Um diesem Umstand gerecht zu werden, haben wir parallel zum Buch eine eigene Webseite www.blockchain4u.ch erstellt. Darauf werden laufend die **neuesten Entwicklungen** zum Thema sowie **Anpassungen** zum Buch gepostet. Zudem wird eine ständig aktualisierte Liste von wichtigen **Internet-Links** publiziert.

Aufgrund der **Neuartigkeit** des Fachgebiets entstehen auch laufend neue Begrifflichkeiten. Die Begriffe werden darüber hinaus je nach Quelle anders definiert und genutzt. Im Buch werden die **verwendeten Begriffe** daher immer definiert und abgegrenzt.

1 Die drei aufgeführten Protokolle eignen sich aufgrund ihrer spezifischen Funktionen und ihrer Bekanntheit, um die wichtigsten Unterscheidungsmerkmale auf der Protokollebene exemplarisch zu erläutern. Es gibt jedoch zahlreiche weitere Protokolle und es kommen auch laufend neue Protokolle hinzu.

2 Dazu zählen vor allem die international tätigen Banken, Versicherungen sowie Unternehmen aus der Informatik-Branche (z. B. IBM, Google, SAP). Aber auch Telekommunikationsanbieter wie die Swisscom oder Warenhausketten (z. B. Walmart) wirken bei aktuellen Blockchain-Projekten mit.

Zudem wird darauf hingewiesen, wo und wann es in der Praxis oder in der Literatur zu Verwechslungen und Missverständnissen kommen kann.

Das Thema Blockchain beschäftigt nicht nur ein deutschsprachiges, sondern ein globales Publikum. Deshalb ist es auch nicht verwunderlich, dass die Mehrheit der Literatur in **englischer Sprache** verfasst ist und die Begrifflichkeiten vom Englischen geprägt sind. Aus diesem Grund werden die **englischen Fachbegriffe** jeweils in Klammern nach den deutschen Begriffen erwähnt.

Rückblick / Zusammenfassung Kapitel 1

In diesem Kapitel wurden folgende zentralen Aspekte behandelt:

- Die Blockchain-Technologie verfügt über diverse Anwendungsbereiche. Kryptowährungen und Tokens sind nur *ein* Anwendungsbereich.
- Die Blockchain-Welt lässt sich in drei Ebenen unterteilen: Technologien, Protokolle und Applikationen.
- Blockchain ist nur *eine* mögliche Ausprägung von verteilten Transaktionssystemen (Distributed Ledger Technology, DLT).