



Kompaktwissen Finanzen 4.0

BLOCKCHAIN IN DER PRAXIS

Funktionsweise und Anwendungsfälle

INHALT

1	Einleitung	<i>Seite 4</i>
2	Begriffe und Funktionsweise im Kontext von Blockchain	<i>Seite 4</i>
3	Vorteile und Chancen durch die Blockchain-Technologie	<i>Seite 7</i>
4	Nachteile und Limitationen beim Einsatz der Blockchain-Technologie	<i>Seite 8</i>
5	Mögliche Anwendungsbereiche	<i>Seite 10</i>
	» Kryptowährungen	<i>Seite 10</i>
	» Banking & Wertpapiergeschäfte	<i>Seite 11</i>
	» Versicherungen	<i>Seite 12</i>
	» Fertigung, Logistik & Handel	<i>Seite 12</i>
	» Musikindustrie	<i>Seite 13</i>
	» Internet der Dinge & Sharing Economy	<i>Seite 13</i>
	» Behörden (national und international) & humanitäre Hilfe	<i>Seite 14</i>
	» Reisen	<i>Seite 15</i>
6	Fazit	<i>Seite 15</i>

IMPRESSUM

Verleger:

ibi research an der Universität Regensburg GmbH
Galgenbergstraße 25
93053 Regensburg
Geschäftsführer: Prof. Dr. Hans-Gert Penzel (Vors.),
Dr. Anja Peters, Dr. Georg Wittmann

Registergericht: Amtsgericht Regensburg
Registernummer: HR Regensburg B 5409
Umsatzsteuer-Identifikationsnummer gemäß § 27 a
Umsatzsteuergesetz: DE 814337479

Telefonnummer: 0941 943-1901
Faxnummer: 0941 943-1888
E-Mail-Adresse: ehr@ibi.de
Website: <https://kompetenzzentrum-augsburg-digital.de>

Soweit keine redaktionelle Kennzeichnung für den Inhalt Verantwortlicher im Sinne des Presserechts und gem. § 55 II Rundfunkstaatsvertrag:
Prof. Dr. Hans-Gert Penzel (Vors.), Dr. Anja Peters, Dr. Georg Wittmann,
Galgenbergstraße 25, 93053 Regensburg

Bildquellen:

© wladimir1804 / fotolia.com (Titelseite)
© Production Perig / fotolia.com (Seite 6)
© 206732962 / stock.adobe.com (Seite 9)
© 197968727 / stock.adobe.com (Seite 13)

Grafische Konzeption und Gestaltung:

zwetschke GmbH & Co. KG
Proviantbachstraße 1¼ • 86153 Augsburg

Text und Redaktion:

Sabine Pur, ibi research an der Universität Regensburg GmbH

ISBN:

978-3-945451-64-9

Stand:

Januar 2019

HAFTUNGSERKLÄRUNG

Das Werk mit seinen Inhalten wurde mit größtmöglicher Sorgfalt erstellt und gibt den zum Zeitpunkt der Erstellung aktuellen Stand wieder. Dennoch kann für seine Vollständigkeit und Richtigkeit keine Haftung übernommen werden.

Interviews und Kommentare Dritter spiegeln deren Meinung wider und entsprechen nicht zwingend der Meinung von ibi research. Bei der Nennung von O-Tönen wurden diese ggf. sprachlich und grammatikalisch ohne den Sinn zu verändern dem Stil der Studie angepasst. Fehlerfreiheit, Genauigkeit, Aktualität, Richtigkeit, Wahrheitsgehalt und Vollständigkeit der Ansichten Dritter können seitens ibi research nicht zugesichert werden.

Die Informationen Dritter, auf die Sie möglicherweise über die in diesem Werk enthaltenen Internet-Links und sonstigen Quellenangaben zugreifen, unterliegen nicht dem Einfluss von ibi research. ibi research unterstützt nicht die Nutzung von Internet-Seiten Dritter und Quellen Dritter und gibt keinerlei Gewährleistungen oder Zusagen über Internet-Seiten Dritter oder Quellen Dritter ab.

Die Angaben zu den in diesem Werk genannten Anbietern und deren Lösungen beruhen auf Informationen aus öffentlichen Quellen oder von den Anbietern selbst.

Bitte beachten Sie, alle genannten Preise sind Momentaufnahmen und können sich jederzeit ändern.

Die Wiedergabe von Gebrauchsnamen, Warenbezeichnungen, Handelsnamen und dergleichen in diesem Werk enthaltenen Namen berechtigt nicht zu der Annahme, dass solche Namen und Marken im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann genutzt werden dürften. Vielmehr handelt es sich häufig um gesetzlich geschützte, eingetragene Warenzeichen, auch wenn sie nicht als solche gekennzeichnet sind. Bei der Schreibweise hat sich ibi research bemüht, sich nach den Schreibweisen der Hersteller zu richten.

Trotz der Vielzahl an Informationen sowie aufgrund einer dem ständigen Wandel unterzogenen Sach- und Rechtslage kann das Werk jedoch keine auf den konkreten Einzelfall bezogene Beratung durch jeweilige fachlich qualifizierte Stellen ersetzen. ibi research empfiehlt deshalb grundsätzlich bei Fragen zu Rechts- und Steuerthemen und rechtsverwandten Aspekten, sich an einen Anwalt oder an eine andere qualifizierte Beratungsstelle zu wenden. Bei Anregungen, Kritik oder Wünschen zu diesem Werk würden wir uns sehr über Ihre Rückmeldung freuen. Schreiben Sie uns an ehr@ibi.de eine E-Mail.

1

EINLEITUNG

Kaum ein IT-Thema geht momentan so stark durch Presse und Medien wie die Blockchain. Weltweit betrachtet entwickelten sich die Venture Capital-Investitionen in diese Technologie von rund 360 Millionen US-Dollar in 2014 auf gut 645 Millionen US-Dollar in 2017,¹ mit weiter steigender Tendenz. Aber bei den mittelständischen Unternehmen scheint das Thema noch nicht so richtig angekommen zu sein. Nach einer Umfrage des eco-Verbandes im Mittelstand haben zwei Drittel der Befragten von dem Thema noch gar nichts gehört. Beim Rest sind es jedoch nur 20 Prozent, die den Einsatz der Blockchain im eigenen Unternehmen nicht näher in Betracht ziehen. Die übrigen 80 Prozent befassen sich zum Teil schon intensiv damit.² Ein Grund für den geringen Bekanntheitsgrad in der Breite des Mittelstands ist das Fehlen eines gemeinsamen Verständnisses über die Technologie, ihre Potenziale und Limitationen sowie die verschiedenen Einsatzmöglichkeiten.

An dieser Stelle soll der vorliegende Leitfaden Abhilfe schaffen und das Thema Blockchain aus praktischer und anwendungsorientierter Sicht genauer beleuchten. Dafür werden zuerst Begrifflichkeiten und Funktionsweise der Blockchain-Technologie erläutert, anschließend wird auf Vor- und Nachteile bzw. Chancen und Limitationen eingegangen, gefolgt von konkreten Einsatzfeldern und Praxisbeispielen.

2

BEGRIFFE UND FUNKTIONSWEISE IM KONTEXT VON BLOCKCHAIN

Was ist eine Blockchain?

Eine Blockchain (dt. Blockkette) ist betriebswirtschaftlich vergleichbar mit einem elektronischen Kassen- oder Hauptbuch. Allerdings gibt es von diesem Buch eine Vielzahl verteilter Kopien. Technisch handelt sich also um eine dezentrale Transaktions-Datenbank (DLT – Distributed Ledger Technology), die in einem (Peer-to-Peer-)Netzwerk³ auf einer Vielzahl von Rechnern (Knoten) in exakt identischer, d. h. gespiegelter Form vorliegt. Die Blockchain in ihrer Implementierung als verteilte Datenbank wurde erstmals im Jahr 2008 von Satoshi Nakamoto (einem Pseudonym) in dessen White Paper zu Bitcoin ausgeführt⁴. Der Datenbestand in Form der Blockchain besteht aus einer linearen Aneinanderreihung von Kettengliedern bzw. Blöcken, die zeitlich nacheinander und logisch konsistent aufeinander aufbauen. Jeder Block beinhaltet neben den eigentlichen Transaktionsdaten u. a. einen Zeitstempel und einen mit kryptographischen

Methoden errechneten Kontroll- bzw. Hashwert dieses Blocks sowie des vorangegangenen Blocks (vergleichbar einer Quersumme).⁵ Bei einer nachträglichen Löschung oder Veränderung der Informationen in einem Block passt der jeweilige Hashwert nicht mehr zu dem Block. Da die Blöcke aufeinander aufbauen, würde der nächste Block nicht mehr konsistent zu seinem Vorgänger sein. Dabei existiert keine zentrale Kontrollstelle mehr. Eine solche Manipulation würde in dem Netzwerk zwischen Rechnern, auf denen die Blockchain ja mehrfach in identischer Form vorliegt und in dem die Transaktionen „gemeinsam“ verifiziert, validiert und neue Blöcke geschaffen werden, nahezu in Echtzeit auffallen. Die Daten, die sich einmal in der Blockchain befinden, können somit nicht mehr verändert oder gelöscht werden. Alle Beteiligten können die Transaktionen in der Blockchain sehen, aber niemand kann sie manipulieren.

Wie werden die Blöcke der Blockchain erstellt?

Jeder neue Block wird in der Regel über ein Konsensverfahren geschaffen und bestätigt; er wird anschließend an die Blockchain angehängt. Das am meisten verbreitete Verfahren ist die Proof-of-Work-Methode (PoW). Um hier einen neuen Block von Transaktionen zu erstellen, wird ein unbekannter zufälliger Wert (Nonce) durch Ausprobieren erraten. Dieser Vorgang wird als „Mining“ bezeichnet: Bekannt sind der Hashwert des neuen Blocks und weitere Daten, wie der Zeitstempel, die Transaktionsdaten und der Hashwert des alten Blocks. Die Nonce stellt die unbekannte Zahl dar, die auch dem neuen Block zugehörig ist und die nun durch Ausprobieren gefunden werden muss. Dabei muss der Miner genau diejenige Nonce finden, die zusammen mit den bekannten gegebenen Daten über einen Hash-Algorithmus den Hashwert des neuen Blocks ergibt. Besonders wichtig an dieser Methode bzw. an der Logik von Hashfunktionen ist, dass es sich um Einwegfunktionen handelt. Ein beliebiger Input wird mittels eines kryptographischen Verfahrens in einen Output transferiert (Hashwert). Dabei ergibt derselbe Input immer denselben Output. Es lässt sich aber nicht vom Output zurück auf den Input rechnen. Da in diesem Netzwerk sehr viele leistungsstarke Rechner gleichzeitig an der Lösung der Gleichung arbeiten, wird ein gewisser Zeitdruck aufgebaut. Denn nur der erste, der das Rätsel löst und damit den neuen Block generiert, erhält als Belohnung Kryptogeld (Coins) also z. B. Bitcoins oder Ether.⁶ Die übrigen Rechner im Netz nehmen dann seine Lösung, rechnen damit die Hashfunktion nach und bestätigen bzw. validieren somit sein Ergebnis und die im Block gespeicherten Transaktionen. Da es sich um ein Konsensverfahren handelt, das für Sicherheit sorgen soll, müssen dieses Ergebnis mehr als die Hälfte der Rechner validieren. Danach wird bei jedem die Aktualisierung der Blockchain abgespeichert.

Ein weiteres Modell, das weniger Energie und Rechenleistung benötigt, ist die Proof-of-Stake-Methode (PoS). Hier werden keine Rätsel durch Ausprobieren gelöst. Zum „Minen“ von Blöcken und Validieren von Transaktionen werden als Basis die von den Minern gehaltenen Coins genommen. Je mehr Coins ein Miner hat, desto mächtiger ist er. Der jeweilige Miner muss einen sog. Master Node im Netzwerk betreiben und einen gewissen Teil seiner Coins als Nachweis einfrieren. Man kann also sagen, dass er einen Teil seines Guthabens als Sicherheit hinterlegen muss und dafür eine Rendite erhält. Diese Methode ist deutlich schneller und besser skalierbar, führt aber zu einer gewissen Oligopolisierung bzw. Zentralisierung, was die Blockchain ja eigentlich vermeiden soll. Hier haben einige wenige mehr Macht als andere; es ist somit kein Netzwerk unter Gleichberechtigten im eigentlichen Sinne mehr. Oftmals findet sich bei den verschiedenen Blockchain-Technologien ein Mix aus PoW und PoS. Es existieren noch andere Verfahren, die aber selten Einsatz finden.

¹<https://de.statista.com/statistik/daten/studie/654326/umfrage/venture-capital-investitionen-in-blockchain-technologien-weltweit>

²https://www.wik.org/uploads/media/PS_PP_2018_04_10_Sicherheit_Blockchain_KMU_01.pdf
https://www.eco.de/wp-content/blogs.dir/20170222_ergebnisse-blockchain-umfrage.pdf

³In einem Peer-to-Peer-Netzwerk arbeiten alle Computer gleichberechtigt zusammen.

⁴Das White Paper kann hier heruntergeladen werden: <https://bitcoin.org/bitcoin.pdf>.

⁵Eine detailliertere Beschreibung der Struktur und Inhalte von Blöcken findet sich beispielsweise hier: <https://www.dev-insider.de/was-ist-ueberhaupt-ein-block-a-638193>

⁶Es kann passieren, dass mehr als ein Rechner glaubt, der Schnellste gewesen zu sein. Aber auch für diesen Konflikt existiert ein Lösungsweg, der allerdings hier nicht weiter beschrieben wird.

Wie offen ist der Zugriff auf die Blockchain?

Es existieren zwei Arten von Blockchains – offene und geschlossene. Die offenen (public) Blockchains sind für jeden öffentlich zugänglich, Ethereum oder Bitcoin sind Beispiele hierfür. Die geschlossenen (private) Blockchains hingegen stehen nur einem bestimmten Teilnehmerkreis zur Verfügung. Sie sind oftmals für Unternehmen interessant, weil hier der Zugriff auf einen ausgewählten Benutzerkreis festgelegt werden kann und somit auch gleich Themen wie Datenschutz, Betriebsgeheimnisse und ähnliches Beachtung finden. Die Linux Foundation treibt unter dem Namen Hyperledger die Blockchain-Technologie auf Open-Source-Basis für das Enterprise-Segment voran. In diesem Konsortium befinden sich Unternehmen wie Daimler, IBM, Intel und SAP.⁷

Was sind Smart Contracts?

Sind in der Blockchain nicht nur Werte, sondern auch ausführbare Programme bzw. Zustände gespeichert, spricht man von Smart Contracts – von programmierbaren intelligenten Verträgen. Bei einer Transaktion werden dann aufgrund der Logik des Programms die Eigenschaften/Attribute eines Objekts und somit sein Zustand verändert. Dabei erfolgt automatisiert eine vorher definierte Aktion auf ein vorher definiertes Ereignis. Voraussetzung ist, dass es sich um vollständige Verträge handelt, bei denen alle Möglichkeiten bzw. Zustände digital abbildbar sind. Smart Contracts können in verschiedenen Bereichen eingesetzt werden. Beispielsweise kann eine Checkliste in einem Genehmigungsprozess von mehreren Parteien hintereinander abgearbeitet werden. Oder diverse Akteure bewegen gemeinsam Güter durch eine Lieferkette, etwa im Außenhandel, und es gibt keinen einzelnen Akteur, der an einer Stelle sämtliche Daten für die anderen Parteien vorhalten könnte. Dies wird in den unten aufgeführten Anwendungsbeispielen noch deutlich.

Was ist Ethereum?

Ethereum bzw. die Ethereum Virtual Machine ist eine umfangreiche Plattform, die auf der Blockchain-Technologie basiert. Sie hat den Einsatzzweck, Smart Contracts zwischen zwei oder mehr Parteien mit Hilfe von verteilten Apps (DApps – Dezentralisierte Applikationen) auszuführen. Die Programmiersprache für die Smart Contracts auf Ethereum ist Solidity. Sie ist den Programmiersprachen C und Java sehr ähnlich und erleichtert so häufig den Einstieg für Programmierer in das Thema. Allerdings ist die Sprache auch limitiert und anderen in einigen Punkten vielleicht unterlegen. Die aktuelle Methode zum Minen ist PoW, bei dem die Miner allerdings die „hauseigene“ Kryptowährung Ether und nicht Bitcoin erhalten. Aber es wird derzeit der alternative Konsensmechanismus PoS unter dem Namen Casper eingeführt.

Die Technologie Ethereum basiert auf einem Positionspapier, das von Vitalik Buterin, dem Leiter der Ethereum Foundation, 2013 verfasst wurde. 2017 wurde die Enterprise Ethereum Alliance gegründet, ein Konsortium, das die Entwicklung von Unternehmensanwendungen auf Basis der Ethereum-Blockchain vorantreibt. Mitglieder sind neben der Ethereum Foundation große Unternehmen wie Cisco und Microsoft aber auch verschiedene Startups.⁸ Ethereum hat sehr großes Potenzial und ein breites Anwendungsfeld. Kein Wunder also, dass hier viele große und kleine Unternehmen gemeinsam forschen. Einige Umsetzungsprojekte sind weiter unten aufgeführt.

» 3 VORTEILE UND CHANCEN DURCH DIE BLOCKCHAIN-TECHNOLOGIE

Der Einsatz einer Blockchain ist gerade dann sinnvoll, wenn Prozesse unternehmensübergreifend, ineffizient und nicht transparent sind. Und wenn bei der Bearbeitung von digitalen oder physischen Gütern, Rechten oder ähnlichem verschiedene Beteiligten involviert sind, ohne dass es die eine, von allen Beteiligten akzeptierte Vertrauenspartei gibt. Sie kann **Transparenz** und **Vertrauen** schaffen und die **Zusammenarbeit effizienter** gestalten.

Das dezentrale System der Blockchain ersetzt die Notwendigkeit einer vertrauenswürdigen zentralen Instanz und macht den Einsatz von klassischen Intermediären überflüssig. Dies hat zum einen den Vorteil, dass dadurch **Transaktionskosten** minimiert werden können. Zum anderen wird durch den Konsensmechanismus die Blockchain von der Community bzw. Crowd verifiziert und nicht von einer einzelnen Instanz. Das – zusammen mit den kryptographischen Verfahren zur Validierung von Transaktionen – macht das System sehr **fälschungssicher**.

Ein weiterer Vorteil der dezentralen Struktur ist, dass sich das System **selbst erhält** und es nicht mit einem einzelnen Unternehmen steht und fällt. Das redundante Vorhalten der Blockchain auf verschiedenen Rechnern in einem verteilten Netzwerk hat ferner den Vorteil, dass der Ausfall einzelner Rechner das Gesamtsystem nicht beeinträchtigt.



⁷ <https://www.hyperledger.org>

⁸ <https://entethalliance.org>



4

NACHTEILE UND LIMITATIONEN BEIM EINSATZ DER BLOCKCHAIN-TECHNOLOGIE

Ein grundlegender Nachteil der Blockchain-Technologie ist ihre **Ineffizienz**. Denn die Blöcke müssen von einer Vielzahl von Parteien in einem aufwendigen Verfahren zunächst parallel gerechnet und dann ebenfalls parallel dauerhaft abgespeichert werden.

Daraus resultiert der häufig diskutierte Nachteil der fehlenden **Skalierbarkeit**. Gerade bei offenen Blockchains ist das Thema kritisch. Denn wenn z. B. immer mehr Anwendungen auf der Ethereum-Blockchain implementiert und eingesetzt werden, droht die Infrastruktur wie ein Flaschenhals zu verstopfen. Daher ist auch bei Ethereum inzwischen ein Umstieg von der PoW- zur PoS-Methode in der Umsetzung, die deutlich effizienter ist.

Ein aktuelles Beispiel zum Thema Skalierbarkeit: Das Unternehmen MotionWerk hat den Service Share&Charge entwickelt, bei dem unter anderem die Abwicklung der Abrechnung von Elektroautos an Ladestationen auf Blockchain-Basis erfolgen sollte. Inzwischen wurde der Dienst insbesondere wegen der mangelnden Skalierbarkeit in Bezug auf die entsprechenden Transaktionskosten eingestellt. Allerdings wurde er in die neu gegründete gemeinnützige Share&Charge Foundation übertragen, dort weiterentwickelt und bereits mehrfach pilotiert.⁹

Die beschriebene Ineffizienz führt zu einem immens hohen **Stromverbrauch**, der beim Minen entsteht und der die Technologie somit umweltschädlich macht. Allein schon die Schaffung von Bitcoins verbraucht fast so viel Strom wie ganz Österreich. Die Miner stellen ihre Serverfarmen in der Regel dort auf, wo der Strom am günstigsten ist. So platzen sie diese zum Beispiel in Schweden, Finnland oder Kanada. Der Strom ist in diesen Ländern so günstig, weil dort ein Überschuss vorhanden ist, der häufig aus erneuerbaren Energien gewonnen wird. Dies scheint das Argument etwas zu relativieren.¹⁰ Andererseits sind nach wie vor die meisten Miner in China tätig, wo sie eine Vielzahl von Kohlekraftwerken auslasten.

Auch wenn das Thema **Sicherheit** bei Blockchains so hervorgehoben und betont wird, so kann es in der IT grundsätzlich nie absolute Sicherheit geben. Die Basis für die Sicherheit in diesem System ist, dass es bisher keinen Algorithmus gibt, der die mathematische Rückwärtsberechnung der Hashfunktion überhaupt bzw. in annehmbarer Zeit lösen kann und reines Ausprobieren zu lange dauern würde. Zudem existieren auch immer wieder Sicherheitslücken, die es möglichst schnell zu schließen gilt, bevor sie missbraucht werden. Die Sicherheitslücken bei Open Source Systemen wie Ethereum werden z. B. in Foren wie Reddit¹¹ diskutiert. Ein weiteres Problem in Bezug auf Sicherheit ist der Faktor Mensch. Je mehr Menschen auf ein System zugreifen können, desto mehr ist die Frage der Sicherheit auch außerhalb der IT, direkt beim Nutzer zu thematisieren.

Auch wenn die dezentrale Technologie klassische **Intermediäre als Sicherheitsinstanz** überflüssig macht, so bedarf es ggf. noch einer dritten Instanz, wie eines technischen Supports. Wenn in solchen Technologien Smart Contracts mit komplexeren Sachverhalten abgebildet werden, wird wahrscheinlich darüber hinaus eine betriebswirtschaftliche Erklärungsinstanz notwendig.

⁹ <https://www.electrive.net/2018/02/23/blockchain-ladenetz-sharecharge-wird-vorerst-beendet>
<https://shareandcharge.com>
<https://medium.com/share-charge/the-next-share-charge-bc5f6807ddd6>
<https://shareandcharge.com/roadmap>

¹⁰ <https://bitcoinblog.de/2018/05/28/warum-der-hohe-stromverbrauch-von-bitcoin-vermutlich-kein-problem-fuer-die-umwelt-ist>

¹¹ <https://www.reddit.com/r/ethereum>

Ein weiterer Aspekt, der kritisch zu beleuchten ist, ist die Qualität der Daten. Die Anwendungen auf der Blockchain können nur so gut sein wie die Daten, auf denen sie basieren. Denn unser momentanes und sehr aktuelles Problem – der oftmals ungenügenden **Qualität der Daten** – löst die Blockchain nicht.

Datenschutz und Datensicherheit ist auch bei der Blockchain ein wichtiges Thema. Es können im System Transaktionen eines Schlüsselpaars (öffentliche und private Schlüssel) beobachtet und analysiert werden, was Rückschlüsse auf die Interaktion verschiedener Partner ziehen lässt. Dies kann gerade bei der Zusammenarbeit verschiedener Unternehmen unerwünscht sein. Zudem sehen europäische Aufsichtsbehörden **bankenaufsichtsrechtliche Probleme** beim Einsatz der Blockchain im Finanzwesen. Hier ergibt sich ein echtes Dilemma: Ein Akteur sollte, wenn er seinen Datenschutz bewahren will, nicht unter seinem Klarnamen agieren. Dieses Verstecken ist aber andererseits unter dem Aspekt „Know Your Customer“ nicht akzeptabel und öffnet der anonymen Finanzierung illegaler Transaktionen Tür und Tor.

Problematisch könnte auch das Thema **„der gläserne Mensch“** sein. Angenommen, ein Mensch würde seine Miete nicht pünktlich überweisen, dann wäre durch den Einsatz von Smart Contracts auf der Blockchain folgendes Szenario denkbar: Es könnten ihm gleich automatisch weitere Services, wie Flugbuchungen und Einkäufe von Luxusgütern vorerst gesperrt werden.

¹² Weitere Informationen zum Schlüsselpaar unter Kryptowährungen.



>> 5 MÖGLICHE ANWENDUNGSBEREICHE

Die Blockchain-Technologie existiert nicht nur in der Experimentierumgebung der IT-Labors von Startups und Großunternehmen. Es gibt bereits Beispiele in der realen Welt, wo sie praktisch eingesetzt wird – meist noch als Beta-Versionen oder in der Pilotierung, aber mit ersten Beispielen auch im Rollout. Nachfolgend sind exemplarisch einige Anwendungsbeispiele aufgeführt, die das breite Spektrum (im Ansatz) aufzeigen sollen, das die Technologie mit sich bringt. Die Aufzählung ist rein zufällig, unvollständig und ohne Wertung.



Kryptowährungen



Banking & Wertpapiergeschäfte



Versicherungen



Fertigung, Logistik & Handel



Musikindustrie



Internet der Dinge & Sharing Economy



Behörden & humanitäre Hilfe



Reisen

Auch wenn Bitcoin fast die Hälfte des Gesamtmarktes an Kryptowährungen ausmacht, so gibt es noch weitere alternative Währungen, so genannte **Altcoins**. Davon existieren derzeit fast 2.000 im Internet. Auf der Webseite <https://coinmarketcap.com> befindet sich eine aktuelle Übersicht. Die derzeit am bekanntesten sind neben Bitcoin **Ether**, die Währung, die auf der Plattform Ethereum beruht, und **Ripple**, die allerdings nicht komplett dezentralisiert ist. Erwähnenswert ist an diesem Punkt noch, dass im August 2017 die Bitcoin-Blockchain gespalten wurde, um deren Effizienz zu steigern, und seitdem zusätzlich die effizientere Währung Bitcoin Cash neben Bitcoin existiert.

Die Stabilität der Altcoins hängt sehr vom Kurs der Bitcoins ab. Da diese eine starke Marktmacht besitzen, „ziehen“ sie quasi die anderen Währungen nach. Im Kursverlauf kann diese Korrelation deutlich nachvollzogen werden. Das digitale Geld wird in einer digitalen Geldbörse, einer so genannten Wallet, aufbewahrt. Es wird dort bei Transaktionen empfangen und von dort versendet. Dafür ist ein digitales Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel notwendig. Der private Schlüssel kann mit der PIN und den TANs beim klassischen Online-Banking verglichen werden, der öffentliche mit der IBAN.¹³

Weitere Informationen:

- » <https://de.statista.com/themen/2087/bitcoin>
- » <http://www.deraktionaer.de/aktie/bitcoin-startet-naechsten-angriff-386760.htm>



Kryptowährungen

Viele Menschen setzen noch immer Blockchain mit **Bitcoin** gleich. Aber Bitcoin ist eine Kryptowährung, die auf der Blockchain-Technologie beruht. Der/die Erschaffer ist/sind unter dem Pseudonym Satoshi Nakamoto bekannt. Im PoW-Verfahren wird den Minern, die als erste den neuen Block generieren, als Belohnung eine bestimmte Anzahl an Bitcoins überlassen. Bitcoin wurde zum einen als Währung zur Abwicklung von Transaktionen geschaffen. Darüber hinaus dient sie als virtuelle Geldanlage und zur Spekulation. Dabei sind die Ausschläge nach oben und unten enorm, die Anlage ist also mit hohen Risiken behaftet.

Mit Bitcoin kann man bereits bei Unternehmen real bezahlen, beispielsweise beim Lieferdienst Lieferando oder beim Reiseportal Expedia. Aber auch vor Ort gibt es Unternehmen, die Bitcoin akzeptieren. Im niederländischen Arnheim existieren bereits über 100 Geschäfte, in denen mit Bitcoins bezahlt werden kann. Übersichten über Bitcoin-Akzeptanzstellen sind etwa unter <https://www.btc-echo.de/bitcoin-akzeptanzstellen> oder unter <http://coinmap.org> zu finden. Zudem kann man beispielsweise auch an mehreren Schweizer Bitcoin-Automaten (Bitcoin ATM) Bargeld in Bitcoins tauschen und umgekehrt.

Weitere Informationen:

- » <https://www.giga.de/downloads/bitcoin/specials/hier-koennt-ih-in-deutschland-mit-bitcoin-bezahlen-mit-liste>
- » <https://www.merkur.de/leben/geld/kann-jetzt-schon-bitcoins-zahlen-zr-8777577.html>
- » <https://www.bitcoinnews.ch/8442/bitcoin-atm-die-schweiz-erhaelt-3-neue-bitcoin-automaten>
- » <https://coinatmradar.com/country/206/bitcoin-atm-switzerland>

Banking & Wertpapiergeschäfte

Theoretisch kann die Blockchain als eine Art Transaktionsregister bei der Abwicklung von internationalen Zahlungen oder Wertpapiergeschäften eingesetzt werden. Eine konkrete und erfolgreiche Umsetzung in der Praxis ist jedoch schwer zu finden. Die Großbank Santander beispielsweise hatte im April 2018 den internationalen Geldüberweisungsdienst **One Pay FX** eingeführt, der auf der Technik XCurrent des Startups Ripple fußt. XCurrent wurde als Blockchain-basierte Technologie vorgestellt. Umgesetzt wurde dort aber lediglich ein bidirektionaler Nachrichtenaustausch. Es hat sich herausgestellt, dass das dezentrale Blockchain-Konzept für den Einsatz in der global vernetzten Finanzindustrie nicht geeignet ist. Im Finanzbereich existieren sehr viele Daten, die verarbeitet werden müssen. Das System hätte einen viel zu hohen Rechenaufwand und könnte nicht skalieren. Zudem wäre der Energieverbrauch immens. Was die Logik des Systems völlig ad absurdum treibt, ist die Tatsache, dass die Kontrolle der Daten durch eine zentrale Instanz, wie eine Bank, hier explizit notwendig bzw. gewünscht wurde.

Weitere Informationen:

- » <http://www.manager-magazin.de/unternehmen/banken/blockchain-ripple-raeumt-schwaechen-der-technik-ein-a-1212968.html>
- » <https://de.cointelegraph.com/news/ripple-banks-unlikely-to-apply-blockchain-for-cross-border-payments-in-near-future>

¹³<https://www.coinpro.ch/public-und-privat-key-beim-wallet-fuer-kryptowaehrungen>





Versicherungen

Fizzy ist eine Anwendung im Beta-Stadium, die auf der Ethereum-Blockchain aufbaut. Es handelt sich hier um eine Police des französischen Versicherungsunternehmens Axa, bei der sich Fluggäste gegen Verspätungen absichern können. Hierbei wird für den Kunden der Kaufvorgang wie auch die Schadensmeldung im Verspätungsfall automatisiert ohne weiteres Zutun des Kunden abgewickelt.

Weitere Informationen:

- » <https://fizzy.axa/en-gb>
- » <https://coincierge.de/2018/versicherungsgigant-axa-veroeffentlicht-produkt-auf-ethereum-blockchain>

Das 2016 gegründete Schweizer Startup **B3i Services AG** wurde vom B3i-Konsortium, das aus 15 globalen Versicherern und Rückversicherern wie Allianz und Generali besteht, gegründet. Ziel ist es, die Effizienz von Versicherungslösungen entlang der Wertschöpfungskette mit Hilfe der Blockchain-Technologie deutlich zu steigern. Dabei steht B3i für „Blockchain Insurance Industry Initiative“. 2017 wurden beim Prototyp für „Property Cat XoL“-Rückversicherungsverträge bereits Effizienzsteigerungen um bis zu 30 Prozent gemessen. Die ersten Live-Transaktionen sind noch 2018 geplant.

Weitere Informationen:

- » <https://b3i.tech/home.html>
- » https://www.allianz.com/de/presse/news/engagement/sponsoring/180326_B3i-Mitglieder-gruenden-Blockchain-Startup



Fertigung, Logistik & Handel

Gerade in der Lebensmittelindustrie, in der die Lieferketten oft über Ländergrenzen hinaus gehen und die Transportwege häufig lang, ineffizient und nicht transparent sind, könnte die Blockchain eine deutliche Verbesserung bedeuten. Alle Beteiligten in der teilweise sehr langen Prozesskette könnten mit einem einzelnen Datensatz arbeiten. Es wäre jederzeit für alle nachvollziehbar, wann die Ware wo ist und, mit entsprechenden Sensoren an den Transportkisten, ggf. auch in welchem Zustand. IBM beispielsweise forscht mit anderen Unternehmen bereits an über 400 Blockchain-Projekten. Eines davon ist **IBM Food Trust**. Hier arbeiten neben Walmart, Nestlé und Dole noch sieben weitere Unternehmen zusammen, um die Sicherheit von Lebensmitteln zu verstärken, Rückrufaktionen frühzeitig koordinieren zu können und Abfall zu reduzieren. Die ersten Tests sind bereits 2017 durchgeführt worden. Walmart sei nach eigenen Angaben nun bereits für den Produktiveinsatz. Eine ähnliche Herangehensweise ist beispielsweise auch beim chinesischen Online-Händler **JD.com** im Einsatz, um Fleisch von Australien bis zum Kunden zu tracken.

Weitere Informationen:

- » <https://de.cointelegraph.com/news/walmart-ibmblockchain-initiative-aims-to-track-global-foodsupply-chain>
- » <https://de.cointelegraph.com/news/walmart-isready-to-use-blockchain-for-its-live-food-business>
- » <https://www.coindesk.com/e-commerce-giant-jdto-launch-blockchain-as-a-service-platform>
- » <https://www.ibm.com/blockchain/solutions/foodtrust>

Musikindustrie

Für die Musikbranche bietet die Blockchain-Technologie neue Möglichkeiten, jeden, der an einem Stück mitgearbeitet hat, adäquat zu vergüten. Das US-Startup **Ujo Music** bietet eine Beta-Version mit Smart Contracts für die Verwaltung von Rechten inkl. Vergütung an die Teil-Eigentümer. Der Musiker legt hier Preis und Verwertungsmodell selbst fest und wird direkt vom Nutzer bezahlt. Dritte Instanzen wie Plattenfirmen oder Musikportale, bei denen oftmals ein Großteil des Geldes bleibt, fallen hier weg. Ein ähnliches Grundprinzip steht hinter **Peer-Tracks** und **bittunes**.

Weitere Informationen:

- » <https://ujomusic.com>
- » <https://www.fuer-gruender.de/blog/2018/03/blockchain-geschaefsideen>
- » <https://peertracks.com>
- » <http://www.bittunes.org>

Internet der Dinge & Sharing Economy

Bei dem Projekt **Slock.it** ging es in erster Linie um selbstverwaltende Haustürschlösser. Hier sollten neben der Internet-of-Things-Kommunikation (IoT) zum Türöffnen auch alle zugehörigen Prozesse beispielsweise bei einer Vermietung einer Ferienwohnung, wie Beauftragung/Reservierung der Wohnung und Bezahlung, über die Ethereum-Blockchain abgewickelt werden. Inzwischen hat sich das Projekt deutlich weiter in die Sharing Economy entwickelt. Es ist vorgesehen, das Teilen von Objekten wie ungenutzten Wohnungen, Büroräumen, Maschinen oder sonstigen Mobilien sowie Immobilien zu vereinfachen. Die Grundidee dahinter ist, Eigentum zu monetarisieren. Ein Beispiel ist auch die Vermietung eines Fahrrades. Ein vernetztes Fahrradschloss kann über die Blockchain geöffnet und das Fahrrad für die Dauer der Nutzung bezahlt werden – das alles ohne Zutun eines Dritten. Das Projekt wurde anfangs von RWE, nun wird es vom Innogy Innovation Lab und von Siemens unterstützt.

Weitere Informationen:

- » <https://slock.it/landing.html>
- » <https://www.btc-echo.de/was-ist-eigentlich-aus-slock-it-geworden>





Behörden (national und international) & humanitäre Hilfe

Das Startup **Bitnation** erschuf 2014 einen Kryptostaat – eine virtuelle Nation mit Weltbürgern. Hier sollen neben Staats- und Verwaltungsakten auch Dienstleistungen, wie das Ausstellen von Heiratsurkunden oder das Schließen von Geschäfts- und Kreditverträgen mittels der Pangea-Software abgewickelt werden. Die Software ist skalierbar und nicht an eine bestimmte Software für Dezentrale Ledger gebunden, verwendet aber derzeit die Ethereum-Plattform.

Weitere Informationen:

- » <https://bitnation.co>
- » <https://www.tokens24.com/de/cryptopedia/coin-guides/was-ist-bitnation>

Das Projekt **BitNation Refugee Emergency Response (BRER)** des Startups Bitnation hat den Best Idea Award 2017 von der UNESCO NETEXPLO gewonnen. Bei diesem Programm sollen Immigranten eine Blockchain Emergency ID bekommen, die als Starthilfe mit einer virtuellen Staatsbürgerschaft, einer digitalen Geldbörse usw. ausgestattet ist.

Weitere Informationen:

- » <https://refugees.bitnation.co>
- » <https://futurism.com/innovative-refugee-project-wins-major-award-for-its-blockchain-solution>

Estland gilt als Vorzeigestaat im Bereich Digitalisierung. Das Land forscht auch im Bereich Blockchain und kooperiert bereits mit Bitnation, um allen Personen unabhängig von ihrer Nation zu ermöglichen, virtuelle Bürger Estlands zu werden. In dem sog. „E-Residency-Programm“ können diese z. B. in Estland online ein Unternehmen gründen und alle Behörden-gänge im Browser erledigen.

Weitere Informationen:

- » <https://e-resident.gov.ee>
- » <https://www.welt.de/wirtschaft/article170098780/In-dieses-Land-koennen-Sie-jetzt-digital-auswandern.html>

Das Münchner Unternehmen Datarella hat für die Vereinten Nationen (UN) 2017 in Jordanien das Pilotprojekt **Building Blocks** zur Kosteneinsparung bei der Verteilung der UN-Finanzhilfen umgesetzt. Im Flüchtlingscamp Tazweed Village bezahlen die Flüchtling ihre Lebensmittel in Form von Essensgutscheinen über ein Blockchain-basierendes Kontensystem und mittels biometrischer Identifikation per Iris-Scan in einem der lokalen Supermärkte. Mit Hilfe dieses Systems können laut UN im Camp fast 4 Millionen US-Dollar jährlich eingespart werden.

Weitere Informationen:

- » <https://datarella.com/building-blocks-how-the-world-food-programme-harnesses-blockchain-technology-to-deliver-aid>
- » <https://www.lead-digital.de/fluechtlingshilfe-via-blockchain>

Reisen

Das Schweizer Startup **Winding Tree** arbeitet an einem dezentralen B2B-Marktplatz für Unternehmen der Reisebranche auf Ethereum-Basis. Das Zusammenbringen von Fluggesellschaften, Hotels und anderen Reisedienstleistern soll den Zwischenhändler eliminieren und mehr Transparenz und Effizienz schaffen. Neben anderen Partnern kooperiert auch die Lufthansa bereits mit dem Unternehmen Winding Tree. Als Währung auf dem Marktplatz ist das Kryptogeld Tif vorgesehen.

Weitere Informationen:

- » <https://windingtree.com>
- » <https://www.heise.de/newsticker/meldung/Lufthansa-beteiligt-sich-an-Blockchain-basiertem-Reisemarkt-Winding-Tree-3860184.html>



Das Thema Blockchain ist mehr als ein Hype. Es hat Potenzial und beschäftigt immer mehr Unternehmen aus verschiedensten Branchen. Die Blockchain kann Vorteile bieten wie höhere Transparenz in den Prozessen, Manipulationssicherheit und Senkung der Transaktionskosten. Dem stehen aber mögliche Nachteile und Limitationen entgegen, insbesondere die Ineffizienz der verteilten IT-Lösung mit Defiziten in der Skalierbarkeit des Systems, hohem Stromverbrauch und aufsichtsrechtlichen Hürden.

Aber bei dem Einsatz der Blockchain-Technologie geht es potentiell um viel mehr. Sie schafft einen Anreiz für strategisches Umdenken in den einzelnen Unternehmen. Initiiert durch eine neue Technologie, aber bei genauerem Hinsehen vor allem aus prozessualer Sicht, ist eine Entwicklung weg von den zentralen Plattform-Modellen hin zu dezentralen Kooperationsmodellen überlegenswert. Wettbewerbsvorteile und Fortschritt werden hier in der Regel über Unternehmens- und Branchengrenzen hinweg realisiert. Immer mehr große und kleine Unternehmen finden sich in Konsortien zusammen, um gemeinsam Anwendungsbereiche zu erschließen und die neuen Möglichkeiten in Pilotprojekten zu erproben. Ob nun in der Sharing Economy, der Musikindustrie, bei der Entwicklungshilfe oder zur Chargenverfolgung – die Einsatzmöglichkeiten sind vielfältig.

Auch wenn sich die meisten Blockchain-Projekte aktuell eher noch in der Konzeptionsphase befinden, so existieren doch erste Anwendungen bereits im produktiven Einsatz. Einer Expertenumfrage von ibi research zufolge sind 80 Prozent der Befragten davon überzeugt, dass Blockchain in den nächsten fünf bis zehn Jahren eine wichtige Rolle einnehmen wird.¹⁴ Was nun diese Technologie in Zukunft alles bringen wird, bleibt spannend. Vielleicht werden auch Lösungen, die durch die Blockchain erst in die Überlegung kamen, am Ende mit klassischen Technologien realisiert. Das Mittelstand 4.0-Kompetenzzentrum Augsburg wird das Thema auf jeden Fall weiter beobachten.

¹⁴<https://www.ibi.de/presseundticker/1563-ibi-blitz-digital-banking-die-blockchain-kommt-nur-der-zeitpunkt-ist-ungewiss.html>



Das Mittelstand 4.0-Kompetenzzentrum Augsburg gehört zu Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationen, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

