# 1 Vom Vertrauen zum Wissen durch Blockchain

Vertrauen ist eine riskante Erfindung der Moderne. Das behauptet die Berliner Forscherin Ute Frevert, die sich in einem großen Forschungsprojekt des Max-Planck-Institutes für Bildungsforschung seit vielen Jahren als Historikerin mit dem Thema Gefühle westlicher Gesellschaften und deren Veränderung auseinandersetzt.[1] Die renommierte Wissenschaftlerin spricht sogar von einer regelrechten *Obsession für das Vertrauen*.[2] Diese Aussage überrascht. Ist es nicht vielmehr so, dass die Menschen schon immer einander vertraut haben? Warum sollte das Ausdruck einer Besessenheit sein? Ohne Vertrauen kann eine Gesellschaft schließlich nicht funktionieren. Wir gehen morgens aus dem Haus und vertrauen darauf, dass unser Auto in der Werkstatt repariert wurde und wir mit ihm sicher fahren können. Wir vertrauen darauf, dass das Essen in der Kantine nicht vergiftet ist, dass die Polizei kommt und uns hilft, wenn wir sie brauchen. Wir vertrauen den Ärzten, wenn wir ihren Rat suchen, und vertrauen unsere Kinder der Kindergärtnerin an. Wird dieses Vertrauen erschüttert, funktioniert unsere Gesellschaft nicht mehr. Zumindest moderne Gesellschaften sind bei Vertrauensverlust in ihrem Kern getroffen. Denn moderne Gesellschaften sind hochkomplexe Gebilde, deren Komplexität geradezu zu Vertrauen *zwingt*. Das jedenfalls sagte einer der größten Soziologen der Moderne, Niklas Luhmann.[3] Selbst bestens ausgebildete Spezialisten, hochgebildete Akademiker müssen blind vertrauen, und zwar *jeden Tag*. Es bleibt ihnen nichts anderes übrig. Denn die vielen Teilsysteme einer Gesellschaft sind viel zu komplex, um sie für Laien – und das sind wir alle auf vielen Gebieten – transparent, verständlich und kontrollierbar zu machen. Die Antwort auf diese Ohnmacht des modernen Menschen lautet: *Vertrauen haben*. Diese immer überfordernde Komplexität moderner Gesellschaften wird durch Vertrauen in das Funktionieren der verschiedenen Teilsysteme wirkungsvoll reduziert und damit für Menschen wieder

handhabbar. Würden wir alles misstrauisch beäugen, was uns umgibt, und alles kontrollieren müssen, wäre unsere Gesellschaft lahmgelegt. Wir können nicht den Kfz-Mechaniker kontrollieren, ob er alles richtigmacht. Dafür fehlen uns Zeit und Kompetenz. Genauso wenig können wir dem Koch im Restaurant ständig auf die Finger schauen oder die Kindergärtnerin stundenlang mit gerunzelten Augenbrauen beobachten, ob sie unseren Filius optimal fördert. Wir sind also auf Vertrauen *angewiesen*.

## Fehlt Vertrauen, droht der Kollaps

Stammesgesellschaften haben dieses Problem nicht. Da kennt jeder jeden und alle sind in die Kontrolle der Gruppe eingebunden. Vertrauen ist hier nicht notwendig. Vielmehr war das Misstrauen der Regelfall, zumindest gegenüber Fremden. Das jedenfalls hat Ute Frevert erforscht.[4] Das Wort ›Vertrauen‹ taucht in historischen Quellen nur im Zusammenhang mit Gott auf. Nur Gott allein schenkte man Vertrauen, vor allem in Krisen wie Hungerzeiten oder Epidemien.[5] Erst mit dem Beginn der Moderne im 17. und 18. Jahrhundert wird Vertrauen zum zentralen Thema. Das ist kein Zufall, denn diese Gesellschaft konnte sich nicht mehr auf Ständeordnungen und Traditionen und deren richtungsweisende Regeln verlassen. Davon hatte der Mensch sich gelöst. Zwar geht auch Frevert von einem angeborenen Grundvertrauen des Menschen aus, aber erst seit die Rechte und Interessen der Menschen durch Gesetz, Polizei und den Staat geschützt sind, wurde es leichter, auch *Fremden* zu vertrauen.[6] Erst der moderne Mensch konnte es sich erlauben, Vertrauen auch Unbekannten zu gewähren, ohne ökonomische Risiko-Nutzen-Abwägung.[7] Das Vertrauen in hochkomplexe Institutionen, das sich in der beginnenden modernen Gesellschaft nicht auf Tradition, sondern auf *Funktion* stützt, wird zur Pflicht oder genauer: *zur Voraussetzung einer modernen Gesellschaft*. Dieses Vertrauen ist kein Vertrauen von Mensch zu Mensch, sondern ein Vertrauen *in das Funktionieren von Systemen*. Was es bedeutet, in einer modernen Gesellschaft

Vertrauen zu verlieren, haben wir in dramatischer Weise erlebt, als die Finanzkrise 2008 über uns hereinbrach. Als Erstes ging die Investmentbank Lehman Brothers pleite. Das hatte niemand für möglich gehalten. Ein gewaltiger Dominoeffekt war die Folge. Plötzlich wollten sich die strauchelnden Banken untereinander kein Geld mehr leihen, tiefes Misstrauen machte sich in der Branche wie ein bösartig wucherndes Krebsgeschwür breit, der Geldfluss kam ins Stocken. Genau wie die Banken entzogen auch die Verbraucher ihren Hausbanken das Vertrauen. Politiker verloren ihr Vertrauen in die Seriosität und das Verantwortungsbewusstsein der Bankvorstände. Der damalige Wirtschaftsminister Peer Steinbrück fühlte sich nach eigenen Angaben bei den Verhandlungen mit den Banken oft so, als ob er »hinter die Fichte geführt werden sollte«.[8] Das Vertrauen in das Finanzsystem war komplett zusammengebrochen. Eine tiefgehende Vertrauenskrise. In einer modernen Gesellschaft bedeutet das: *eine existenzielle Krise*. Wer Vertrauen zerstört, zerstört die Hauptschlagader der modernen Gesellschaft. Es kostete vor allem den Steuerzahler Milliarden, inklusive größter Verluste bei Renten und Lebensversicherungen, diesen Vertrauensverlust einigermaßen wieder ins Lot zu bringen und damit den totalen Kollaps zu verhindern. Genau darauf, »too big to fail zu sein«, hatten die Finanzakrobaten gesetzt. Es hatte funktioniert. Bis heute mussten die Banken das geliehene Geld nicht zurückzahlen, wohingegen es für die Bankkunden nach wie vor selbstverständlich ist, ihre Kredite abzubezahlen. Kein Wunder also, dass auf Seiten des Verbrauchers bis heute das Misstrauen geblieben ist, zumal die Krise nach wie vor nicht behoben ist, solange die faulen Kredite im Markt sind. Und das sind sie noch immer.[9] So dramatisch die Finanzkrise auch von allen empfunden wurde, so war sie trotz allem nur der Beinahezusammenbruch eines *Teilsystems* der Gesellschaft, des Finanzsektors, wenn auch mit heftigsten Auswirkungen auf die Wirtschaft. Doch dieses Erlebnis führte eindringlich vor Augen, wie essenziell das Vertrauen in einer modernen Gesellschaft ist, vor allem in der Wirtschaft. Vertrauen ist das Schmiermittel, das dafür sorgt, dass das Getriebe

einer Gesellschaft reibungslos funktioniert, vergleichbar mit dem Motorenöl, das den Automotor am Laufen hält.

## Die Geburt des Bitcoins

Krisenerfahrungen machen Menschen kreativ und so erhob sich aus den Trümmern der Finanzkrise die erste virtuelle Währung mit dem Namen *Bitcoin*, was so viel bedeutet wie *digitale Münze*. Unter dem geheimnisvollen Pseudonym Satoshi Nakamoto, bei dem bis heute nicht entschlüsselt werden konnte, wer dahintersteckt, ob es sich dabei um eine Person oder eine Gruppe handelt, wurde 2008, genau zu Halloween, ein White Paper mit dem Titel »Bitcoin: A Peer-to-Peer Electronic Cash System« ins Netz gestellt.[10] Ein Zahlungsmittel, das von Computer zu Computer transferiert werden kann, ohne Zwischenschaltung von Banken. Zunächst blieb das brisante Papier unbemerkt. Schließlich waren alle mit der Pleite von Lehman und deren Verwerfungen beschäftigt. Zwei Monate später folgte nach der Bitcoin-Ankündigung die Software. Wahrscheinlich wäre das Ganze in der breiten Bevölkerung unbemerkt geblieben, wären da nicht die Notenbanken gewesen, die eine Liquidität in den Markt pumpten, bei der nicht nur Laien schwindelig wurde. Die Summen, die täglich, manchmal stündlich, transferiert wurden, hatten derart viele Nullen, dass das Vorstellungsvermögen schlicht überfordert wurde. Ganz offensichtlich handelte es sich um eine Mund-zu-Mund-Beatmung für einen schwer komatösen Patienten. Das sollte die Banken retten und das Finanzsystem irgendwie am Leben halten. Damals wusste keiner, ob das funktioniert. Zweifel gibt es bis heute. Selbst acht Jahre nach der Finanzkrise wurden 2015 von EZB-Chef Mario Draghi immer noch 60 Milliarden Euro *pro Monat* in den europäischen Finanzmarkt eingeschleust.[11] Bis zum Ende seiner Amtszeit 2019 nahm Draghi den Fuß nicht runter vom Pedal der Niedrigzinsen und veranlasste, dass diese Politik auch nach seinem Abgang unter Christine Lagarde weiterläuft.[12] Die Corona-Krise hat

das Problem weiter verschärft. Ein Ende der Niedrigzinspolitik ist in weite Ferne gerückt. Doch Finanzexperten warnen, dass neben den Risiken, die eine solche Politik der Europäischen Zentralbank unter anderem für Sparer, Unternehmer und die staatliche Ausgabenpolitik mit sich bringt,[13] auch die faulen Kredite von einst in Höhe von rund 759 Milliarden Euro nach wie vor im Markt sind.[14]

## Renten werden gekürzt

Am amerikanischen Markt lief die Sache nicht anders. Auch dort wurde der Finanzmarkt mit billigem Geld geflutet.[15] Einer aber muss die Rechnung am Ende bezahlen. Das ist meistens der Steuerzahler. Genau so kam es. Die Rentenprognosen wurden drastisch zurückgefahren, allein im Jahr 2008 verloren die privaten Pensionsfonds weltweit im Schnitt 28 Prozent an Wert.[16] Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) wies 2009 eindringlich darauf hin, dass die öffentlichen Rentensysteme das gleiche Los ereilen würde.[17] Das ist in der Zwischenzeit geschehen. Das Max-Planck-Institut für Sozialrecht und Sozialpolitik schlussfolgerte aus den Zahlen von 2008-2017 ein stark erhöhtes Risiko für Altersarmut.[18] Doch nicht nur die Rentenprognosen wurden herabgesetzt. Am 4. Juli 2014 beschloss der Bundestag, vermutlich nicht ganz zufällig im Schatten der Fußballweltmeisterschaft, die vom Geschehen ablenkte, dass die Renditen der Lebensversicherungen der Situation auf dem Zinsmarkt ›angepasst‹ werden sollten.[19] Im Klartext: Die Kunden der Lebensversicherer bekamen von nun an erheblich weniger Geld, als sie bei Vertragsschluss annehmen durften. Fortan wurden sie nicht mehr zur Hälfte an den Bewertungsreserven bei festverzinslichen Wertpapieren beteiligt.[20] Stille Reserven sollen nur noch in dem Maße ausgeschüttet werden, wenn die Garantiezusagen für die restlichen Versicherten ebenfalls gesichert sind.[21] Das führte dazu, dass beispielsweise ein Versicherungsnehmer, der dagegen klagte und vor Gericht verlor,

am Ende statt 2800 Euro aus den Bewertungsreserven nur noch 150 Euro ausgezahlt bekam.[22] Kein Wunder, dass Finanzexperten diese Vorgänge rund um Renten und Lebensversicherungen zugunsten der Verursacher der Finanzkrise als den »größten Raubzug in der Geschichte« bezeichneten.[23]

## Plötzlich wird Bitcoin interessant

Diese Entwicklungen machte das White Paper von Nakamoto hochinteressant. Die Idee, virtuelles Geld zu entwickeln, das von Banken unabhängig ist, nahm Fahrt auf und ließ die Gemeinde der Bitcoin-Jünger anschwellen.[24] Langsam, aber stetig. Die Rettung schien in der virtuellen Welt zu liegen, weil die analoge Finanzwelt versagt hatte. Der wachsende Erfolg des Bitcoins konnte am Kursverlauf abgelesen werden. Konnte man im Herbst 2010 noch für nur 40 Dollar 500 Bitcoins kaufen (der Einstieg wäre heute rund 1,8 Millionen Euro wert),[25] so musste man im Dezember 2013 schon deutlich mehr hinblättern: 945,74 US-Dollar für einen Bitcoin.[26] Doch kurz darauf kam es zum bisher größten Skandal bei der Bitcoin-Tauschbörse Mt.Gox in Tokio, auf der rund 70 Prozent der damaligen Transaktionen mit Bitcoin stattfanden.[27] Über Nacht waren 850 000 Bitcoins verschwunden, die zu dem Zeitpunkt einen Wert von rund 500 Millionen Dollar hatten.[28] Das war der bisher größte Hack an digitalen Münzen in der Geschichte des Bitcoins.[29] Der Franzose Mark Karpelès, der die Tauschbörse 2011 gekauft und selbst gemanagt hatte,[30] versicherte zwar immer wieder, er habe damit nichts zu tun, er sei beklaut worden und suche ebenfalls nach den digitalen Münzen.[31] Doch viele blieben skeptisch und verdächtigten den jungen Mann, dabei selbst die Hand im Spiel gehabt zu haben. Der ›Baron des Bitcoin‹, wie er einst genannt wurde, kam dennoch glimpflich davon. Die japanischen Behörden verurteilten ihn auf Bewährung wegen Manipulation von elektronischen Aufzeichnungen, die Untreuevorwürfe wurden jedoch fallen gelassen.[32] 200 000 Bitcoins

wurden später in einer virtuellen Geldbörse wiedergefunden. Diese Bitcoins wurden genutzt, um Gläubiger zu entschädigen. Es blieben 160 000 Bitcoins übrig, die zu 88 Prozent immer noch Karpelès gehörten. Im Frühjahr 2018 waren die rund eine Milliarde Dollar wert.[33] Damit war die Kryptobörse Mt.Gox dank des enormen Kursanstiegs nicht mehr insolvent. Doch auf das Geld wollte der Baron großzügig verzichten, alles andere fände er »geschmacklos«, wie er in seinem Blog verlautbarte.[34] Ob es sich dabei um echte Reue und den ehrlichen Versuch von Wiedergutmachung handelte oder um die vorgetäuschte Großzügigkeit eines sehr intelligenten und höchst geschickten Betrügers wird sein Geheimnis bleiben. Immerhin sind die restlichen 650 000 Bitcoins, die nicht wiedergefunden wurden, heute rund 3,8 Milliarden Dollar wert.[35]

## Vertrauenskrise bei den Bitcoin-Jüngern

Dieser Hack bei Mt.Gox bedeutete in der Bitcoin-Gemeinde eine Zäsur. Hatten doch viele von ihnen in der digitalen Münze den Heilsbringer von morgen gesehen. Und nun das: die erste große Vertrauenskrise. Die Geschichte hinterließ einen fahlen Nachgeschmack. Doch sie war nicht das Ende des Bitcoins. Und auch nicht das Ende spektakulärer Hacks, bei denen große Mengen Bitcoins plötzlich auf mysteriöse Weise verschwanden. Die bisher Letzte auf der Liste der Hacker-Trophäensammlung war die weltgrößte Bitcoin Börse Binance, die, wie CEO Changpeng Zhao zuvor nicht müde wurde zu betonen, nicht zu knacken sei.[36] Die Realität widerlegte ihn. Das Diebesgut: 7000 Bitcoins. Zwar wurden bisher nie mehr so viele Bitcoins gestohlen wie bei Mt.Gox, doch es war klar: Die Tauschbörsen hatten ein Sicherheitsproblem.[37] Vertrauen geht anders. Dabei fokussierte sich der Vertrauensverlust nicht allein auf das Sicherheitsproblem. Die privaten Schlüssel, die den Zugang zu den digitalen Geldbörsen regeln, den so genannten Wallets, können immer gestohlen werden, wenn sie nicht sicher genug aufbewahrt

werden. Worauf sich die Augen der Bitcoin-Gläubigen richteten, waren die auffälligen Ups and Downs des Bitcoin-Kurses. Ein Kursverlauf, der spätestens seit 2017 sehr ›volatil‹ war,[38] wie es an der Börse im Fachjargon heißt. Eine Studie des New Yorker Blockchain-Forschungsunternehmens Chainalysis Inc. machte deutlich, worum es dabei ging: Die Coins wurden tatsächlich nur selten als Zahlungsmittel genutzt, sie waren zum reinen Spekulationsobjekt mutiert.[39] Was Zweifel bei den Bitcoin-Anhängern hervorrief, waren nicht der Bitcoin selbst, sondern die Art und Weise, *wie* mit dem Bitcoin umgegangen wurde und bis heute umgegangen wird. Damit ist die Kryptowährung meilenweit weg von der ursprünglichen Intention des Erfinders Nakamoto, eine neue Währung zu etablieren, die unter anderem genau solche Spekulationsblasen verhindern sollte.

## Datenabzocke erschüttert Vertrauen

Doch nicht nur mit dem Diebstahl von virtuellem Geld hat das Internet zu kämpfen, auch der massenhafte Identitätsklau ist ein leidvolles Thema, das wertvolles Vertrauen verspielt. Ein Vertrauensverlust, der für eine moderne Gesellschaft bedrohlich ist, zumal deren digitaler Umbau mitten im Gange ist. Vor zehn Jahren titelte der Fernsehsender ntv auf seiner Webseite »Wilde Zeiten. 2009. Das Jahr der Datenskandale«.[40] Der größte Skandal war dabei der Angriff eines jungen Hackers, dem es gelungen war, 1,6 Millionen Userdaten bei SchülerVZ abzuziehen.[41] Zehn Jahre später ist das bereits Peanuts. Da lautete die Schlagzeile: »Millionen Passwörter im Netz veröffentlicht«.[42] Ein Konglomerat aus 773 Millionen gestohlenen E-Mail-Adressen und 21 Millionen Passwörter wurden frei zugänglich ins Netz gestellt.[43] Der Datenklau verzeichnete eine steile Kurve nach oben. Doch dieser Kursanstieg war kein Gewinn wie an der Börse, sondern ein Verlust, bei dem das Vertrauen der Kunden in den Keller rutschte. Der bisher größte Datenklau aber geschah 2013 bei Yahoo. Daten von drei Milliarden Yahoo-Konten

wurden gehackt.[44] Betroffen von Datenabzocke waren nicht nur die großen Konzerne wie Yahoo, auch die kleinen und mittleren Unternehmen wurden in Mitleidenschaft gezogen. Jedes zweite mittelständische Unternehmen wurde bereits Opfer.[45] Ein Ende ist nicht in Sicht. Der Identitätsklau wurde ein ständiger Begleiter der digitalen Gesellschaft.

## Daten als Geschäftsmodell

Weiteres wertvolles Vertrauen wurde verspielt, als der illegale Datenaustausch der großen IT-Konzerne aufflog. Allen voran: Facebook. Inzwischen hat das Unternehmen sich einen unrühmlichen Namen beim Datenhandel gemacht. Doch Facebook schaut auf sein Geschäftsgebaren mit ganz anderen Augen. Der Datengigant brüstet sich damit, weltweit 2,5 Milliarden Menschen miteinander zu vernetzen.[46] Dabei entstehen Daten in einer sozialen Tiefe, die nicht nur Marketingstrategen Tränen des Glücks in die Augen treiben, sondern auch Geheimdienste neidisch werden lassen. Die Verbraucher aber sind sauer wegen der illegalen Abzocke ihrer privaten Daten, vor allem in Deutschland. Facebook steht am sozialen Pranger. Immer wieder taucht der Name Facebook auf, wenn es im großen Stil um Datenverkauf oder Datennutzung im Graubereich geht. So etwa bei dem Skandal um Cambridge Analytica.[47] Als Facebook-Kunden die App ›thisisyourdigitallife‹ nutzten, hatten viele von ihnen geglaubt, sie unterstützten mit ihren Daten die wissenschaftliche Forschung. Tatsächlich aber erstellte Cambridge Analytica Psychogramme der Facebook-Kunden und verkaufte diese Daten an politische Strategen. Solche Daten sollen Trump zum Sieg verholfen haben. Damit jedenfalls prahlte der ehemalige Chef von Cambridge Analytica, Alexander Nix.[48] Kurz darauf wurde er gefeuert. Nach dem Fernsehinterview war klar: So werden scheinbar harmlose Daten zur politischen Waffe. Es ist sicher kein Zufall, dass der rechtspopulistische Stephen Bannon, einst Chefstratege von Trump, Vizepräsident in dem Unternehmen

war, das inzwischen Konkurs angemeldet hat.[49] Vermutlich war die Berichterstattung, nachdem die Sache aufgeflogen war, doch nicht so gut fürs Geschäft. Doch das bedeutet nicht, dass damit dem illegalen Datenhandel ein Riegel vorgeschoben ist. Wo das eine Unternehmen Konkurs anmeldet, wird woanders einfach ein neues Unternehmen gegründet. Die neue Firma Emerdata ist laut eigener Beschreibung ebenfalls in der Datenverarbeitung tätig.[50] Möglicherweise war die Schließung von Cambridge Analytica bloß ein raffinierter Schachzug, um die Geschäfte nun mit neuem Namen weiterführen zu können.

## Cambridge Analytica und die Folgen

Es geht also bei Facebook nicht nur darum ›Menschen miteinander zu verbinden‹, wie das in Kalifornien ansässige Unternehmen immer wieder betont, sondern im Wesentlichen darum, mit diesen Daten eine Menge Geld zu verdienen. Was andere mit den Daten machen, interessiert den Zuckerberg-Konzern offenbar nicht. So flüsterten eingeweihte Whistleblower der englischen Zeitung *Guardian*, dass der Populist und Anti-Europäer Nigel Farrage mit Cambridge Analytica zusammengearbeitet haben soll, das wiederum die Facebook-Daten zu nutzen wusste.[51] Auch Boris Johnson steckte demnach 40 Prozent seines Wahlkampfgeldes in ein kanadisches Unternehmen, das wiederum eng mit Cambridge Analytica arbeitete.[52] Es ist daher davon auszugehen, dass dieses Datenwissen auch beim Brexit eine große Rolle gespielt hat. Das ist zwar noch nicht alles bis ins Letzte belegt, aber die Recherchen der Investigativjournalistin Carole Cadwalladr haben eine Menge ans Tageslicht gebracht.[53] So weiß Cadwalladr, dass es einen noch nicht namentlich genannten amerikanischen Milliardär gab, der mit seiner Firma beim Brexit-Referendum half, in Großbritannien »den größten konstitutionellen Wechsel des Jahrhunderts« herbeizuführen.[54] Mit diesen Fragen und auch mit der, inwieweit die Russen die Anti-Europa-Kampagnen im Vorfeld des Brexit massiv beeinflusst haben, hat sich ein

Untersuchungsausschuss in London befasst, dessen Ergebnisse Boris Johnson jedoch unter Verschluss hält.[55] Nun ist auch dem Letzten klar: Die Kontrolle über unsere Daten haben wir längst verloren. Denn Facebook hat nicht nur mit jenem ominösen Unternehmen Cambridge Analytica das ganz große Rad beim Datenhandel gedreht, auch mit Giganten wie Yahoo und Netflix betrieb es jahrelang ähnliche Deals.[56] Irgendwann aber packten ehemalige Mitarbeiter bei der *Washington Post* aus und nannten mehr als 150 Firmen, mit denen der Zuckerberg-Konzern solche Geschäfte betrieben hatte.[57] Amazon, Spotify, Microsoft, Apple – alle profitierten davon.[58] Geld floss angeblich nicht, man half sich gegenseitig beim Wachstum und dafür brauchte man die Daten.[59] Mit diesen Daten können die Datenkonzerne die Kunden viel präziser ansprechen. Je individueller die Werbung auf den User angepasst ist, desto mehr Geld lässt sich mit den Klicks verdienen.

## Auch Identitäten werden geklaut

Als der Skandal öffentlich bekannt wurde, machte sich bei den Kunden der Tech-Riesen Unsicherheit breit, aber auch eine gewisse Resignation. Wer am digitalen Leben teil haben will, so glaubten und glauben immer noch viele, müsse wohl diese Nachteile in Kauf nehmen. Doch das Vertrauen, dass ihre Daten dort gut aufgehoben sind, ist dahin. Dabei ist es nicht nur der Verkauf ihrer privaten Daten, der viele Nutzer hat misstrauisch werden lassen, auch die Tatsache, dass immer wieder spektakuläre Hacks offenbaren, dass die Daten in den Clouds von Microsoft & Co. vor fremdem Zugriff nicht sicher sind, verunsichert die Kunden.[60] Offenbar zu Recht. Denn niemand weiß, was alles mit den Daten gemacht wird, wenn sie entwendet oder kopiert werden. Identitätsklau ist dabei ein großes Thema. Sind die Identitäten der Kunden erst einmal in die falschen Hände geraten, können Kontobewegungen manipuliert, falsche Personalausweise ausgestellt oder massenhaft Waren bestellt werden, die der eigentliche Inhaber der Identität im Zweifelsfall bezahlen muss. Dann muss

Strafanzeige gestellt und die Bank informiert werden. Und zwar rasch. Sonst kann es teuer werden bis hin zur privaten Insolvenz.[61]

## CEO-Fraud macht die Runde

Von professionellem Identitätsklau sind auch Führungspersönlichkeiten in Unternehmen betroffen. Ermittler nennen das ›CEO-Fraud‹. Doch das läuft ein wenig raffinierter. Dazu werden soziale Kontakte des CEOs im Netz ausgespäht, die Mitteilungen zu künftigen Investments auf der Unternehmenswebseite verfolgt und vieles mehr. So sind die Täter bestens informiert. Sie wissen, wo sich die Führungskräfte befinden, nutzen etwa deren Auslandsaufenthalt, um mit Hilfe einer gefälschten E-Mail-Adresse oder einem Telefonat in der Buchhaltung Zahlungen auf andere Konten umzuleiten.[62] Meist erzeugen sie künstlichen Zeitdruck, damit nicht zu viel nachgedacht wird. Dass das funktioniert, zeigen die Zahlen. Der CEO-Fraud verursachte allein in Nordrhein-Westfalen im Jahr 2017 einen Schaden von 8,9 Millionen Euro. 2018 lag er bei 6,8 Millionen Euro.[63] Und das sind nur die offiziellen Zahlen eines einzigen Bundeslandes. Die Dunkelziffer wird um ein Vielfaches höher geschätzt. Dabei sind die Betrüger flexibel. Erst waren die Großunternehmen im Visier, jetzt sind es die mittelständischen Betriebe, denn die Großen sind sicherheitstechnisch inzwischen gut geschützt. Praktisch ist für die Betrüger auch, dass bei mittelständischen Unternehmen die Entscheidungswege kürzer sind. Manchmal gibt es nur ein oder zwei Leute im Unternehmen, die manipuliert werden müssen. So haben sie leichteres Spiel.[64]

## Big Brother is watching you

Das Ausspähen von Unternehmen und Bürgern geht allerdings nicht allein auf das Konto von Betrügern. Das erfuhr die Öffentlichkeit im Jahr 2013. Da informierte uns ein sich auf der

Flucht befindlicher unauffälliger junger Mann namens Edward Snowden darüber, dass es ein weltweites virtuelles Spionagenetz gibt, die so genannten ›five eyes‹, in denen sich die amerikanische National Security Agency (NSA), der britische Geheimdienst Government Communications Headquarters (GCHQ) sowie die Geheimdienste von Kanada, Australien und Neuseeland austauschen.[65] Verblüfft nahm die Öffentlichkeit zur Kenntnis, wie weit das Ausspähen geht und wer alles abgehört wird. Dass darunter zahllose Regierungschefs sind, große Organisationen wie Weltbank und Opec, und auch bei Bundeskanzlerin Angela Merkel aufmerksam mitgehört wurde, überraschte weniger als die Tatsache, dass es auch ganz unbescholtene Bürger und Unternehmen trifft, und zwar millionenfach.[66] Die Unterlagen von Snowden enthüllten, dass deutsche, norwegische, spanische und französische Bürger fleißig abgehört wurden.[67] In den USA traf es sogar *alle* US-Bürger im Zeitraum von 2001-2015, bis zu dem Zeitpunkt, als Sektion 215 des Patriot Act ausgelaufen war.[68] Politisch brisant für Europa ist, dass auch der belgische Telekommunikationsanbieter Belgacom abgehört wurde, zu dessen Kunden das EU-Parlament, die EU-Kommission und der Europäische Rat gehören.[69] Unter den ganzen Spionageaktivitäten ist aber vor allem das Muscular-Programm beachtenswert. Das Programm ist in der Tat sehr muskulös, wie der Name bereits vermuten lässt. Denn im Rahmen dieses Programms hackte sich die NSA direkt in die Verbindung der Rechenzentren von Yahoo und Google.[70] Dort speichern die Unternehmen die Daten ihrer Nutzer in so genannten ›Clouds‹. Diese virtuellen Datenwolken sind überall in der Welt verteilt, unter anderem lagern sie in Rechenzentren in Singapur, Taiwan, Hongkong, Irland, Finnland, Chile.[71] In diesen Clouds wird so ziemlich alles gespeichert: E-Mails, Suchanfragen, Videos, Fotos, aber eben auch: Unterlagen von Unternehmen. Viele global agierende Unternehmen nutzen die Clouds, damit Mitarbeiter und Kunden auf die gleichen Datensätze zugreifen können. Das macht das weltweit vernetzte Arbeiten erheblich leichter.

## Die Daten werden vor der Verschlüsselung abgegriffen

Bemerkenswert ist in dem Zusammenhang, dass genau auf den Leitungen, die die NSA infiltrierte, die Daten zwischen den verschiedenen Standorten der Rechenzentren routinemäßig abgeglichen werden. Verschlüsselt werden sie erst dann, wenn die Daten abgerufen werden. Der Ansatz der NSA ist also äußerst effektiv, denn die Daten müssen nicht erst aufwändig geknackt werden.[72] Nach Angaben von Edward Snowden werden jeden Monat etwa 500 Millionen Kommunikationsvorgänge aus Deutschland abgegriffen.[73] Naiv zu glauben, dass dabei nicht auch deutsche Unternehmen betroffen wären. Unangenehm zu wissen, dass private Dinge in unseren Mails, WhatsApp-Nachrichten und SMS auf der anderen Seite des Atlantiks mitgelesen und politisch wie kommerziell intensiv genutzt werden, bei Unternehmen aber zielt es meistens direkt ins Herz der unternehmerischen Tätigkeit. Wer deren Daten gezielt abfängt und auswertet, ist bestens darüber informiert, was die Unternehmen planen, wie sie agieren, mit wem sie kooperieren und an welchen Projekten sie arbeiten. Das nennt man auch *Wirtschaftsspionage* und bietet denen, die das betreiben, einen klaren Wettbewerbsvorteil. Nach Einschätzung von Experten beschert das der deutschen Wirtschaft einen Schaden von rund 4,2 Milliarden Euro jährlich.[74] Betroffen sind Großkonzerne, Autohersteller und ihre Zulieferer sowie Unternehmen, die sich um Aufträge bemühen, die über 200 Millionen Dollar liegen.[75] Die amerikanischen Geheimdienste sind auch überall dort anzutreffen, wo es um höchst aussichtsreiche, so genannte disruptive Technologien geht.[76] Die Spionage betrifft daher nicht nur Großkonzerne, sondern auch innovative mittelständische Betriebe.[77] Dass die NSA bei dem massenhaften Datenabgriff nicht nur die Terrorabwehr im Sinn hat, sondern auch Wirtschaftsgeheimnisse anderer Nationen gezielt stehle, gab Michael Hayden, der die NSA von 1999 bis 2005 leitete, unumwunden zu.[78] Und Glenn Greenwald, jener Journalist, der die Unterlagen von Snowden veröffentlicht hatte,

zog bei seiner Anhörung vor dem Europäischen Parlament ein beängstigendes Fazit: Die Überwachungsprogramme der NSA und seines britischen Partners GCHQ liefen darauf hinaus, dass es bei elektronischer Kommunikation schlechthin keine Privatsphäre mehr geben werde.[79] Nun ist auch dem Letzten klar: Unsere Daten im Internet sind nicht sicher.

## Fake News und die Suche nach der Wahrheit

Neben allen faszinierenden Dingen, die uns das Internet bietet, und auf die wir ungern wieder verzichten würden, hat das virtuelle Netz auch dunkle Seiten und dazu zählt die mangelnde Sicherheit unserer Daten. Es gibt noch einen weiteren Sündenfall, dem das Internet Vorschub leistet. Es sind die Fake News, die uns das Leben im Netz schwermachen. Authentische Daten werden zu einem raren Gut. Auch das ist für eine moderne Gesellschaft, die auf Vertrauen basiert, eine schwerwiegende Belastung. Zwar sind Fake News keine Erfindung des Internets, deren weltweite Verbreitung aber wäre ohne das Internet undenkbar. Darüber hinaus sind sie oft raffiniert gemacht und im Internet gut gestreut. Selbst für Nachrichten-Profis ist es heute eine Herausforderung, Fakten von Fake News zu trennen, vor allem unter Zeitdruck.[80] Und Zeitdruck ist in Nachrichtenredaktionen immer, weil das Internet so schnell ist und Fakten-Checks Zeit kosten. Wie sehr wir falschen Nachrichten ausgesetzt sind, wurde spätestens nach dem amerikanischen Wahlkampf von Donald Trump 2016 deutlich. Russische Trolle hatten massenweise Fake News vor allem über Facebook abgesetzt und Trump damit im Wahlkampf entscheidend unterstützt.[81] Damit wurde etwas sichtbar, was im postkommunistischen Osteuropa aus langer leidvoller Erfahrung längst bekannt war: die Unterwanderung der Medien, heute des Internets, von russischer Desinformation. Dabei helfen ›Medienunternehmen‹ wie die in St. Petersburg ansässige »Internet Research Agency«.[82] Die Medienagentur wurde – und wird vermutlich noch immer – von einem Freund

Putins, dem Oligarchen Jewgenij Prigoschin, massiv finanziell unterstützt.[83] Darin produzieren überwiegend Studenten in Zwölf-Stunden-Schichten unter vielfachen Pseudonymen rund 160 gefälschte Blogbeiträge pro Tag.[84] Lohn der Arbeit: rund 700-900 € im Monat.[85] Für Studenten in Russland viel Geld. Auch diese Erfahrung der massenhaften Verbreitung von Fake News war in der weltweiten Internetgemeinde ein veritabler Schock, hatte man doch im anfänglichen digitalen Hype geglaubt, dass man durch das Internet an bessere, sprich, wahre Originaldaten käme. *Ungefiltert. Ohne Zensur durch die herkömmlichen Medien*. Auch diese Hoffnung wurde zerstört. Und zwar gründlich. Heute wissen wir, dass im Internet nicht nur massenhaft Trolle herumgeistern, sondern intelligente Computer, so genannte Bots, sogar Nachrichten produzieren, die selbst gewissenhaft recherchierende Journalisten in die Irre führen können und Nachrichtentrends produzieren, die es ohne sie gar nicht gäbe.[86]

## Deep Fakes sind täuschend echt

Und als wäre das nicht schon genug, gibt es auch noch das Problem mit den ›Deep Fakes‹.[87] Dabei handelt es sich um Foto-, Film- und Videosequenzen, die mit Hilfe von Künstlicher Intelligenz (KI) bearbeitet werden. Diese Bearbeitungen dank KI machen es möglich, Menschen Aussagen und Handlungen unterzuschieben, die sie nie gesagt oder begangen haben. Besonders infam: Dafür werden nicht nur ihre Konterfeis genutzt, auch ihre Stimmen werden missbraucht. Das fühlt sich für die anderen ziemlich echt an. Nun wird es schwer für die Betroffenen, das Gegenteil zu beweisen. Da tut sich ein Abgrund auf. Die Dinger werden immer besser, immer authentischer. Das birgt die Gefahr, dass irgendwann gar nichts mehr für wahr gehalten wird und nur noch *Meinungen* zählen – völlig losgelöst von den Tatsachen. Genau vor dieser Gefahr hat Hannah Arendt, eine der größten politischen Theoretikerinnen des 20. Jahrhunderts, gewarnt.[88] Wenn alle glauben, dass sowieso nur noch gelogen wird, *nichts mehr*

*wahr ist,* ist der Nährboden für Diktaturen bereitet, weil die Wirklichkeit entgleitet.[89] Dann ist die Demokratie angezählt wie ein angeschlagener Boxer im Ring. Die Verunsicherung aufgrund von Fake News ist inzwischen groß und so fragen sich immer mehr Menschen: *Was ist wahr? Was ist Fake?*

## Blockchain als Lösung

Diese tiefgreifende Vertrauenskrise in die Echtheit von Daten und deren Sicherheit im Netz, ließ den Hunger nach fälschungssicheren, nicht manipulierbaren Daten enorm steigen. Das führte dazu, dass die ursprüngliche Idee von Satoshi Nakamoto wie Phönix aus der Asche auferstand. Nun aber mit einem grundsätzlich veränderten Blickwinkel. Die Aufmerksamkeit richtete sich jetzt weniger auf die Bitcoins als auf die darunterliegende Blockchain-Technologie. Schließlich war sie von ihrem Erfinder Nakamoto erschaffen worden, um fälschungssichere und korrekte Transaktionen von Computer zu Computer zu ermöglichen (Peer-to-Peer). Diese veränderte Perspektive brachte Erstaunliches zutage. Man erinnerte sich, dass diese Datenbank nicht bloß für virtuell erzeugtes Geld genutzt werden kann, sondern für Daten *aller Art*. Man erinnerte sich auch daran, dass die Blockchain-Technologie vor Fälschungen sicher ist. Sind die eingestellten Daten korrekt, ist deren Integrität auf der Blockchain garantiert. Der Grund dafür ist einfach: Wenn ein Schwarm von Menschen jeweils mit Hilfe ihrer Computer bestätigt, dass die Daten aus dem mathematischen Block, der ihnen zugestellt wurde, echt ist, ist es für Manipulatoren schlichtweg unmöglich, alle Teilnehmer zu manipulieren. Die Echtheit wird also nicht von vertrauenswürdigen Einzelpersonen oder Institutionen – einem Notar oder einer Bank – bestätigt, sondern von *vielen*. Und bei jeder Transaktion wird sie erneut bestätigt. Damit bekommen die Daten die Qualität einer Urkunde, ohne dass die Informationen noch verbrieft werden müssen. Ein Schwarm, der sich dezentral auf Millionen von Computern verteilt. Das klingt irgendwie

nach Schwarmintelligenz und ist es auch: Der Schwarm lässt sich nicht täuschen; zumal alle Daten dauerhaft und konsistent dokumentiert sind und diese Wahrheit *dezentral* organisiert ist. Ein Zentrum kann man angreifen, hacken, zerstören, ausradieren. Die Vielen nicht. Wenn die Wahrheit auf so vielen Computern zu finden ist, ist Manipulation nutzlos. Der Mathematiker und Kryptograph Professor Rüdiger Weis bestätigt, dass es in absehbarer Zeit mathematisch nicht möglich sei, die digitalen Ketten zu sprengen.[90] Selbst Quantencomputer, an denen nicht nur Google arbeitet, seien noch lange nicht in der Lage, das Blockchain-System zu knacken, sagt auch Bitcoin-Entwickler Peter Todd.[91] Klar ist aber auch, dass dies irgendwann der Fall sein wird. Deswegen muss die technologische Entwicklung jeweils Schritt halten. Sicherheitsfragen können nie eine letzte Antwort haben.

## Blockchain soll die Industriedaten schützen

Angesichts des derzeitig massiven Datenklaus und der alltäglichen Datenmanipulation brauchen wir dringend eine Technologie, die uns vor dem unbefugten Zugriff auf unsere Daten schützt. Vor allem die Unternehmen in Europa. Professor Weis bringt die derzeitige Situation mit viel Sarkasmus auf den Punkt, wenn er sagt, dass derjenige, der unverschlüsselt kommuniziere, auch gleich seine Daten an die ausländischen Geheimdienste schicken könne.[92] Kein Wunder, dass der Handlungsdruck für die Unternehmen enorm ist. Aber noch aus einem anderen Grund muss dringend etwas gegen den Datenklau getan werden. Daten, deren Authentizität zweifelhaft ist, bedrohen die moderne Gesellschaft, deren Getriebe ins Stottern gerät, wenn nicht mehr vertraut werden kann, weil so viel Fake im Umlauf ist. Dies gilt in ganz besonderem Maße für die Wirtschaft. Der weltweite Handel braucht verlässliche Zahlen und Fakten. Sonst lassen sich keine Geschäfte machen. Zwar sind die privaten Daten

vor dem Zugriff der riesigen US-Datenkraken schon seit geraumer Zeit nicht sicher, dieser Kampf ist verloren, für den Schutz unserer Industriedaten aber lohnt es zu kämpfen. Blockchain könnte dabei eine große Rolle spielen. Denn die Technologie macht nicht nur die Daten erheblich sicherer, sie kann auch deren Echtheit garantieren. Wenn die Anfangsdaten korrekt sind, bleiben sie es auch auf der Blockchain. Niemand kann sie noch manipulieren. *Diese Daten sind wahr*. Wie es um die Wahrheit bestellt ist, ist zudem für jeden der Geschäftsteilnehmer zu jeder Zeit einsehbar. Wer aber die Wahrheit hat, braucht kein Vertrauen. Das Wissen um die Integrität der Daten ersetzt das Vertrauen. Das ist *radikal neu*. Das hat es so noch nie gegeben. Vor allem nicht in der Wirtschaft. Es ist nicht übertrieben, dies einen historischen Umbruch zu nennen.

> *»Wer die Wahrheit hat, braucht kein Vertrauen. Das Wissen um die Integrität der Daten auf der Blockchain ersetzt das Vertrauen.«*

Im Unterschied zum institutionellen Vertrauen des modernen Menschen, der generell darauf vertrauen muss, dass das System Wirtschaft funktioniert und ihm die Waren und Dienstleistungen bietet, die er braucht – selbst in Corona-Zeiten –, war Handel treiben ohne Vertrauen noch nie möglich. Doch das Vertrauen ist von anderer Art. Dieses Vertrauen war immer ein *persönliches* Vertrauen. Eins von Mensch zu Mensch. Nicht umsonst formulierte einst der amerikanische Öl-Tycoon Jean Paul Getty jene Worte, die zum geflügelten Sprichwort wurden: Wenn man einem Menschen trauen kann, erübrigt sich ein Vertrag. Wenn man ihm nicht trauen kann, ist ein Vertrag nutzlos.[93] Das Gleiche drückt das Kaufmannsehrenwort aus, dass in den Hansestädten immer so wichtig war und ohne jenes die Hansestädte wohl nie so reich geworden wären. Vertrauen

als Grundlage für Handel und Wirtschaft. Bis heute wird das Ehrenwort des Kaufmanns in Hamburg hochgehalten.[94] Ein Wort, ein Mann und ein millionenschweres Geschäft wird mit bloßem Handschlag besiegelt.[95] Dieses persönliche Vertrauen ist essenziell. Schließlich kann beim Geschäftemachen eine Menge schiefgehen: Die Ware kommt nicht oder wird nicht pünktlich geliefert, sie hat nicht die Qualität oder Quantität, die vereinbart wurde, das Geld wird nicht zum vereinbarten Zeitpunkt überwiesen oder im schlimmsten Fall bleibt die Zahlung ganz aus. Und das ist nur ein kleiner Ausschnitt aus dem, was alles nicht funktionieren kann. Mit verheerenden Folgen für den, der dem Falschen vertraut hat. Und weil sich das nie geändert hat, gibt es in jeder Kultur regelrechte Zeremonien des Vertrauensaufbaus: Eine Empfehlung öffnet die Tür, man geht miteinander essen, beobachtet den Geschmack und die Manieren seines Gegenübers, tastet im Gespräch einander vorsichtig ab, ist Gastgeber und baut langjährige Geschäftsfreundschaften auf. Man beginnt mit einem kleineren Geschäft, um zu testen, ob es klappt, und weitet sodann schrittweise den Handel miteinander aus. Das hat sich seit dem Altertum bis heute nicht geändert, weil es nie Ersatz für dieses Vertrauen gab. Doch dieses Vertrauen, das im Grunde genommen eine Wette auf die Zukunft ist, ein Vorschuss, bei dem man nie wissen kann, ob er sich auszahlt, weil man in den Kopf des anderen nicht hineinschauen kann, braucht man nun nicht mehr. Dieser seit Beginn der Menschheit praktizierte Vertrauensvorschuss im Handel mit seinem hochkomplizierten Beziehungsgeflecht kann in naher Zukunft im internationalen Warenverkehr zu den Akten gelegt werden. *Wie kann das sein?* Die Frage ist rasch beantwortet. Weil die Daten, die über die Ware präzise Auskunft geben, auf der Blockchain fälschungssicher gespeichert und für die Zugriffsberechtigten jederzeit einsehbar sind. Jeder, der an einem Geschäft beteiligt ist, das über Blockchain abgewickelt wird, kann in wenigen Sekunden in Echtzeit erkennen, wie viel Ware vorhanden ist, welche Qualität sie hat, was sie kostet, wo sie sich befindet und wem sie gehört.[96] *Wer braucht da noch Vertrauen?*

## Vertrauen wird durch Wissen ersetzt

Was diese nahezu tektonische Verschiebung in der Wirtschaft bedeutet, welche Fragen dabei noch ungelöst sind und wie die Suche nach Antworten auf Hochtouren läuft, wird in den folgenden Kapiteln dargestellt. Was allerdings mit einer modernen Gesellschaft geschieht, deren Grundpfeiler auf dem Vertrauen fußt und dieses Vertrauen in vielen Bereichen nun überflüssig wird, können wir noch gar nicht abschätzen. Wir wissen noch nicht, was es für eine Gesellschaft bedeutet, *vom Vertrauen zum Wissen zu wechseln*. Es wird vielleicht sogar noch grundsätzlicher sein als das, was momentan durch die Digitalisierung in der Wirtschaft geschieht, weil es eben das *ganze* System der Moderne erfasst. Dieser Sprung in eine echte Wissensgesellschaft, die das Vertrauen nicht mehr braucht, *weil sie die Wahrheit kennt*, wird sich jedoch nur dann realisieren, wenn zu der Erfindung und dem Hunger nach fälschungssicheren und wahren Daten noch etwas hinzukommt. Es braucht den entscheidenden Treiber, der die Entwicklung voranbringt. *Dieser Treiber sorgt dafür, dass sich die neue Technologie weltweit verbreitet und etabliert.* Ohne einen solchen Treiber bleiben die technologischen Erfindungen aufregende Ideen, an die sich aber bald schon niemand mehr erinnern wird. Sie geraten einfach in Vergessenheit, weil kaum jemand sie nutzt. Wenn aber eine Industrie mit enorm viel Marktmacht sich dieser Erfindung annimmt, kommt es zum Durchbruch am Markt. Diese Rolle fällt der Chemieindustrie zu. Das mag einige überraschen, weil viele die Chemieindustrie gar nicht auf dem Schirm haben, schauen die meisten doch beim Thema disruptive Technologien in Richtung Silicon Valley oder Finanzindustrie, die das Thema Blockchain bisher vorangetrieben hat. Die Chemieindustrie hat jedoch ein Pfund, mit dem sie wuchern kann. Als eine der ganz wenigen Industrien ist sie mit der *gesamten produzierenden Industrie* vernetzt, sie steht mit ihren Produkten am Anfang vieler Lieferketten – und zwar weltweit. Wenn ein solcher Player mit ins Spiel kommt und die Blockchain-Technologie in das Herz seiner globalen IT-Prozesse einpflanzt, dann wird es ernst. Denn

die Geschäftspartner und Kunden, die sich auf allen Kontinenten verteilen, *müssen mitgehen*. Genau diese Entscheidung ist in der Chemieindustrie gefallen. Drei der Blockchain-Pilotprojekte werden in diesem Buch vorgestellt: Themis, Circularise PLASTICS und ReciChain. Namhafte Player der Branche sind dabei: BASF, Covestro, Evonik. Im Mittelpunkt der Pilotierungen steht die Frage, wie sicher und effizient die Warenprozesse und der Zahlungsverkehr auf der Blockchain durchgeführt werden können. Die bisherigen Ergebnisse sind so überzeugend, dass die Industrie in den Startlöchern steht. Die Europäische Kommission in Brüssel reagiert darauf und ebnet der Blockchain mit der European Blockchain Service Infrastructure (EBSI)[97] den Weg *(siehe dazu Interview mit Pēteris Zilgalvis, Head of Unit, Digital Innovation and Blockchain EU-Commission in Kapitel* 6*)*. Fehlt nur noch das digitale Geld für die Zahlungsabwicklung auf der Blockchain (siehe dazu Kasten 2 in Kapitel 2, ›Hinter den Kulissen‹). Dann können die Lieferketten in gar nicht mehr so ferner Zukunft vollautomatisch ablaufen. Da trifft es sich gut, dass die Europäische Zentralbank seit Oktober 2020 den Einsatz des digitalen Euros in einem Pilotprojekt testet. Wenn dieser Probelauf positiv ausfallen sollte, und davon ist auszugehen, steht dem flächendeckenden Einsatz dieser bahnbrechenden Technologie nichts mehr im Weg.

### Öffentliche Blockchain versus Private Blockchain

Die Blockchain muss man sich als eine riesige digitale Datenbank vorstellen, in die prinzipiell jeder digitale Informationen einstellen kann. Diese Informationen können Daten jeglicher Art sein: Rechnungen, Zertifizierungen, Bilder, Dokumente, aber eben auch digitales Geld, wie etwa Bitcoin. Neu ist, dass diese Datenbank nicht zentral verwaltet wird, sondern dezentral von allen Teilnehmern der Blockchain, die Nodes (Knoten) genannt werden. Deren Aufgabe ist es, die in der Blockchain *codierten Daten* zu bestätigen, ohne den Inhalt

zu kennen. Dafür müssen sie aufwändige mathematische Rechenaufgaben lösen (Proof of Work-Methode, kurz PoW-Methode). Die PoW-Methode benötigt viel Energie und Zeit, gilt aber auch als sehr sicher. Wenn die Rechenaufgabe gelöst ist, gelten die eingestellten Informationen als bestätigt und der neue Datenblock wird an die Blockchain angehängt. Daher kommt auch der Name: eine technologische Kette, die aus unzähligen Blocks besteht, die mathematisch miteinander verbunden sind. Die Vorteile der Blockchain liegen klar auf der Hand: Die Daten, die in Hashs verschlüsselt sind, sind wahr, nicht manipulierbar, sicher und transparent. Sie sind transparent, weil sie von allen Teilnehmern zu jeder Zeit in Echtzeit einsehbar sind, sofern sie die Berechtigung dazu haben. Die Daten sind wahr, weil alle auf den gleichen Datenstamm bei den Berechnungen zurückgreifen, vorausgesetzt die Anfangsdaten wurden überprüft und entsprechen den Tatsachen. Sie sind unmanipulierbar, weil jegliche Veränderung auf der Blockchain zurückverfolgt werden kann. Die Daten sind darüber hinaus sicherer als beispielsweise in einer zentralen Cloud. Eine Manipulation der Daten durch Hacker macht wenig Sinn, weil die Wahrheit der Datenhistorie auf unzähligen Computern dezentral gespeichert ist.

#### Private Blockchain

Die private Blockchain ist die von der Industrie bevorzugte Variante. Bei ihr gibt es, anders als bei der öffentlichen Blockchain, Zugangsberechtigungen. Da nicht jeder teilnehmen kann, wird sie auch als private Blockchain bezeichnet. Teilnehmer sind in der Regel die Geschäftspartner. Die bestätigen die eingegebenen Daten in einer weniger aufwändigen Rechenmethode, die Proof of Stake-Methode, kurz PoS. Diese Methode verbraucht wenig Energie, ist sehr schnell, dafür aber auch weniger sicher als die PoW-Methode. Dadurch ist die private Blockchain erheblich schneller als die öffentliche

Blockchain, effizienter und verbraucht weniger Energie. Sie ist daher für die Wirtschaft nützlicher als die öffentliche Blockchain. Die Industrie verbindet mit dem Einsatz der privaten Blockchain unter anderem das Ziel, Lieferketten vollautomatisieren zu können. Für Blockchain-Hardliner mit einem radikal-demokratischen Ansatz ist unter anderem die Einschränkung des Teilnehmerkreises nicht akzeptabel.