ZfdG

Zeitschrift für digitale Geisteswissenschaften

Beitrag aus:
Sonderband 4 der ZfdG: Die Modellierung des Zweifels – Schlüsselideen und -konzepte zur graphbasierten Modellierung von Unsicherheiten. Hg. von Andreas Kuczera, Thorsten Wübbena und Thomas Kollatz. 2019. DOI: 10.17175/sb004

Titel:
Blockchain – die etwas andere Datenbank

Autor/in:
Katarina Adam

Kontakt:
katarina.adam@htw-berlin.de

Institution:
Hochschule für Technik und Wirtschaft Berlin

GND:
1082051918

DOI des Artikels:
10.17175/sb004_009

Nachweis im OPAC der Herzog August Bibliothek:
1037074483

Erstveröffentlichung:
24.04.2019



Letzte Überprüfung aller Verweise:
24.04.2019

GND-Verschlagwortung:
Blockchain | Netzwerkdatenbanksystem | Transaktion |

Zitierweise:
Katarina Adam: Blockchain – die etwas andere Datenbank. In: Die Modellierung des Zweifels – Schlüsselideen und -konzepte zur graphbasierten Modellierung von Unsicherheiten. Hg. von Andreas Kuczera, Thorsten Wübbena und Thomas Kollatz. 2019 (= Sonderband der Zeitschrift für digitale Geisteswissenschaften, 4). PDF Format ohne Paginierung. Als text/html abrufbar unter DOI: 10.17175/sb004_009.

Katarina Adam

# Blockchain – die etwas andere Datenbank


## Abstracts

Trotz vieler Artikel, Berichte und Aufmerksamkeit in den Massenmedien ist die Blockchain-Technologie für die meisten verbunden mit Begriffen wie Bitcoin, Risiko, Spekulation, hohe Volatilität und auch der dunklen Seite des Internets. Das Potential der Technologie wird bei diesen teilweise emotional geführten Diskussionen außer Acht gelassen. Um einen kleinen Beitrag zur Versachlichung zu leisten, ist dieser nachfolgende Aufsatz geschrieben. Es wird erläutert, in welchem Umfeld diese Technologie implementiert wurde, welcher geniale Ansatz hinter der Technologie steht, wie der aktuelle Entwicklungsstand ist und wie die Blockchain Technologie von anderen Ansätzen der Datenspeicherung und -bearbeitung lernen kann. Hierzu wird die Graphdatenbank herangezogen und es werden beide Ansätze verglichen.

Despite many articles, reports and attention in the meantime in the mass media, blockchain technology is for most associated with bitcoin, risk, speculation, high volatility and also the dark side of the Internet. The potential of the technology is ignored in these sometimes emotional discussions. In order to make a small contribution to objectification, this following essay is written. It explains the environment in which this technology has been implemented, the ingenious approach behind the technology, the current state of development and how the blockchain technology can learn from other approaches to data storage and processing. For this the graph database is used and both approaches are compared.


## 1. Siegeszug der Blockchain-Technologie!?

Spätestens mit dem Siegeszug der wohl berühmtesten Krypto-Währung Bitcoin hat die dahinter liegende Blockchain-Technologie den sogenannten Mainstream erreicht. Fast tagtäglich überbieten sich die Medien darin um, mal mit Schreckens-, mal mit Erfolgsgeschichten, über diese Technologie zu schreiben. Blockchain-Technologie gehört als ein Bestandteil zu dem großen Thema Digitalisierung. Und unbestritten ist das dieser Technologie zugesprochene disruptive Potential. Bis sich dieses Potenzial jedoch in Gänze entfalten kann, wird es noch einige Zeit dauern. Ein Grund mehr, sich mit dem Potenzial und den vielfältigen Anwendungsmöglichkeiten auseinanderzusetzen und auch den Vergleich zu anderen Datenbanken nicht zu scheuen. Es kann und darf lebhaft diskutiert werden, ob es sich mit der Blockchain-Technologie um einen Paradigmenwechsel handelt.

Nachfolgend wird zunächst darauf eingegangen, in welchem Umfeld diese Technologie entstanden ist und was die Einzigartigkeit der Erfindung Blockchain ausmacht. Anschließend werden die Eigenschaften der Technologie am Beispiel der ersten Applikation, dem Bitcoin, dargelegt. Die technische Weiterentwicklung macht auch vor der Blockchain-Technologie nicht halt. Daher werden die Ansätze der nachfolgenden Generationen besprochen. Die Blockchain-Technologie ist ein sehr mächtiges Werkzeug, dessen Anwendung mit einigen Beispielen illustriert wird, um die extreme Bandbreite der Anwendungsmöglichkeiten und damit das Potential dieser Technologie erahnen zu können. Die berechtigte Frage, warum

sich weltweit die Projekte noch immer in bestenfalls der Beta-Testing Phase befinden, wird im Fazit beleuchtet. Zuvor wird jedoch der Vergleich zwischen graphbasierten Datenbanken und blockchainbasierten Datenbanken gewagt.

## 2. Volkswirtschaftliche Retroperspektive – oder, wie alles begann

Um die Blockchain-Technologie richtig einordnen zu können, ist es hilfreich, sich noch einmal zurückzuversetzen in das Jahr 2008, als die Finanzkrise, die ihren Ursprung in den USA nahm, wie ein Flächenbrand um den Globus zog. Ökonomen ziehen hier gern die Parallele zur Großen Depression Ende der 20er Jahre des letzten Jahrhunderts.[1]

Vor der großen Finanzkrise gab es auf dem amerikanischen Häusermarkt eine Flut von – im Nachhinein unverantwortlichen – Hypothekenkrediten, begleitet von einem Versagen der Finanzaufsicht und -regulierung.

Um das Ausmaß der Krise zu verstehen, bedarf es eines weiteren Schritts zurück in die Vergangenheit. Das 9/11-Attentat löste eine Schwemme an Geldern aus, um sowohl die Wunden aus den Attacken als auch denen aus dem Platzen der Dotcom-Blase Anfang der 2000er Jahre zu überwinden. Amerika befand sich in einer Rezession und der damalige Vorsitzende der amerikanischen Zentralbank (FED), Alan Greenspan, entschied sich aus Furcht vor einer Deflation zur Politik des billigen Geldes. Dieses billige Geld ermöglichte Geringverdienern (sog. Sub-Prime-Kreditnehmer), sich Wohnungseigentum anzuschaffen. Die kreditbasierte Nachfrage nach Immobilien war in den Folgejahren des Attentats ungezügelt und Häuserpreise schossen in die Höhe.[2] Durch geschickte Bündelung der Kredite (sogenanntes Pooling) entstanden wiederum auf Seiten von Banken völlig neuartige und bestenfalls bedingt einer Regulierung unterworfene Investitions-Produkte. Produkte, die vielfach nicht mehr von den eigentlichen Bankern verstanden wurden, weil algorithmusgetriebene Berechnungen neue Standards und Methoden ermöglicht hatten.[3] Grob gesagt führte die Annahme, dass die Häuserpreise so schnell nicht sinken können, die Niedrigzinspolitik, die den Hunger der Investoren auf Rendite in immer risikoreichere Segmente führte, das Pooling von verschiedenen Krediten sowie das Versagen der Regulierungs- und Aufsichtsbehörden zum Zusammenbruch des Finanzmarktes.[4] Dieses eigentlich lokal auf die USA begrenzte Phänomen konnte sich deshalb in einer Art Dominoeffekt um den Globus bewegen, weil die neu geschaffenen Finanzprodukte weltweit an sowohl institutionelle als auch vermögende Einzelinvestoren veräußert worden waren. Und damit ist die amerikanische Sub-Prime-Krise verantwortlich für eine bis heute anhaltende Finanzkrise, die im Herbst 2008 als prominentes Opfer die Investmentbank Lehman Brothers in die Insolvenz trieb.

[1] Vgl. Sinn 2010, S. 19.
[2] Vgl. Mallaby 2016, S. 596, 597.
[3] Vgl. Bloss et al. 2009, z. B. S. 69 ff.
[4] Vgl. Bloss et al. 2009, z. B. S. 69 ff.

Zu diesem Zeitpunkt mussten weltweit die Zentralbanken intervenieren und in die Märkte eingreifen, um den völligen Kollaps zu verhindern. Nicht verhindern konnten die Zentralbanken, dass zuvor Gewinne privatisiert wurden, nun aber in der Krisenzeit Steuergelder herhalten mussten, um das Bankensystem und damit auch die Wirtschaft am Leben zu erhalten.

In diesem wirtschaftlichen Umfeld ist erstmalig die Blockchain-Technologie auf den Markt gekommen. Die Intention des Erfinders Satoshi Nakamoto (bis heute ist ungeklärt, wer hinter dem Pseudonym steht) war und ist die Abschaffung von Mittelsmännern, die ein System wie das Bankensystem verlangsamen, verteuern und ineffizient halten. Mit einem sogenannten Peer-to-Peer-Netzwerk (p2p) sind diese Mittelsmänner nicht mehr nötig, Zahlungen können digital ebenso abgewickelt werden, wie es bei Barzahlungen mit den herkömmlichen Währungen, z. B. Dollar, Euro, Yen (sogenanntes Fiat-Geld)[5] möglich ist.[6]

Dabei ist die Schaffung einer digitalen Währung kein neuer Ansatz, denn bereits in den 90er-Jahren haben u. a. Nick Szabo (Bit Gold, 1998) und Wei Dai (B-Money, 1998) die ersten Ansätze zu digitalen Währungen veröffentlicht:

Kurz nachdem das B-Money-Whitepaper veröffentlicht wurde, startete Nick Szabo ein sehr ähnliches Projekt namens Bit Gold. Dieses elektronische Währungssystem hatte sein eigenes Proof-of-Work-System, das sich nicht allzu sehr von dem unterscheidet, wie Bitcoin heute geprägt wird. Alle Lösungen wurden kryptographisch zusammengestellt und für die Öffentlichkeit zugänglich gemacht, ähnlich dem Blockchainansatz, den wir heute kennen. Noch wichtiger ist, dass Bit Gold das erste Konzept war, das sich von den zentralisierten Behörden entfernt hat, um doppelte Ausgaben (Double Spending-Problem) der Währung zu vermeiden. Es ist einfach, digital Vorliegendes zu kopieren und ein weiteres Mal zu verwenden; dies kann ein Dokument, ein Song, ein Foto und auch eine digitale Währungseinheit sein, die kopiert und ein weiteres Mal genutzt wird. Dies gilt es jedoch zu verhindern, um Vertrauen in eine digitale Währung zu schaffen. Betrugspräventionen und Fälschungssicherheit ermöglichen dieses Vertrauen, das durch die gesellschaftlich-staatliche Ordnung der herkömmlichen Fiat-Währungen und die dahinterliegende Unabhängigkeit der Geld schaffenden Zentralbanken in der Realwelt vorhanden ist. [7]

Szabos Ziel war es, die Eigenschaften von Gold wiederherstellen, indem er den Zwischenhändler ganz ausschaltete. Man könnte sagen, dass Bit Gold und Bitcoin nicht allzu unterschiedlich sind, obwohl sie mehr als zehn Jahre auseinander liegen.[8]

Digicash, entworfen von David Chaum, war die erste Art von elektronischem Geld, die durch die Verwendung von kryptographischen Protokollen Anonymität bot. Zur Zeit der Entwicklung war Digicash ein revolutionäres Konzept. Durch die Verwendung von

[5] Fiat ; lateinisch für ›*es werde*‹, Fiat-Währung sind Währungen ohne intrinsischen Wert.
[6] Vgl. Nakamoto 2008, S. 1.
[7] Vgl. Chohan 2017, S. 1
[8] Vgl. Szabo 2005.

Kryptographie mit öffentlichem und privatem Schlüssel konnte jeder seine eigene Bank werden und seine Gelder ohne Aufsicht durch Dritte kontrollieren. Ausgegebene Zahlungen wären für Banken und Regierungen nicht nachvollziehbar gewesen. Leider hat das Unternehmen hinter Digicash 1998 Konkurs angemeldet und ist letztlich 2002 verkauft worden. Es ist offensichtlich, dass Digicash ein spannendes Konzept war, aber eben seiner Zeit weit voraus.[9]

All diese Arbeiten an digitaler Währung haben dazu beigetragen, dass der Bitcoin entworfen werden konnte. Mit Hilfe eines Proof-of-Work-Algorithmus für die Generierung und Verteilung neuer Münzen sind viele Funktionen der Vorgänger in das von Satoshi Nakamoto entwickelte Bitcoin-Protokoll eingeflossen. Was die Besonderheit des Ansatzes von Satoshi Nakamoto aus- und damit überlebensfähig macht, ist zum einen die Lösung von Problemen des Double Spending und zum anderen die Vorgabe, nur valide Transaktionen, die die Zustimmung der Mehrheit haben, auf der Blockchain zu speichern.

Da die Blockchain-Technologie nicht mehr nur als interessanter Anwendungsfall für digitale Währungen verstanden wird, und mittlerweile jede Industrie sich bemüht zu verstehen, wie sie mittels dieser Technologie Prozesse verschlanken und vereinfachen kann, wird in diesem Zusammenhang auch von der Distributed-Ledger-Technologie (DLT) gesprochen. Beide Begriffe werden gern synonym verwendet und in beiden Fällen handelt es sich um eine Art Kassenbuch, in dem sämtliche Transaktionen festgehalten werden.

Nachfolgend werden zunächst die Eigenschaften der Bitcoin-Blockchain erläutert. Das Hauptaugenmerk der Bitcoin-Blockchain gilt dem Finanzsektor und den dazugehörigen Finanztransaktionen. Die darauf aufbauenden Versionen oder Generationen adressieren weiterführende Konzepte.

## 3. Eigenschaften einer Blockchain

> » *Die* Blockchain ist zunächst eine große, jedoch dezentrale Datenbank. Zu den Besonderheiten, die die Technik bzw. Datenbank auszeichnet, gehört, dass eine valide Transaktion nicht rückgängig gemacht werden kann, sämtliche Transaktionen transparent und schnell sind, keine zentrale Instanz benötigt wird und alle Transaktionen durch kryptografische Verschlüsselung sicher sind. Bei den Transaktionen, die mittels Blockchain abgewickelt werden können, kann es sich praktisch um jede Form der Übertragung handeln.«[10]

Zu den Details: Viele der Komponenten der Bitcoin-Blockchain existierten schon vorher (s. o. digitale Währung), doch mit der Bitcoin-Blockchain wurden die relevanten Schwachstellen überwunden. Digitales lässt sich einfach kopieren und immer wieder verwenden. Ein fataler

[9] Vgl. Anonymus 1999.
[10] Vgl. Adam 2017, S. 74 ff.

Fehler, wenn es sich um eine digitale Währung handeln soll, denn genau wie eine Fiat-Währung soll die digitale Währung die Tausch-, Rechen- und Aufbewahrungsfunktion erfüllen, um Verbreitung zu erlangen. Diesen Anforderungen genügt der Bitcoin im gewissen Maße.[11]

Warum diese Funktionen trotz aller Einschränkungen so gut sind, liegt vielleicht auch daran, dass es Satoshi Nakamoto u. a. mit seinem Bitcoin-Protokoll gelang, das in der IT-Welt bekannte Phänomen der Byzantine Fault Tolerance zu lösen. Das Bitcoin-Protokoll basiert auf Hashcash für den Proof-of-Work (PoW),[12] Byzantine Fault Tolerance für verteilte Netzwerke sowie der Blockchain als Kette miteinander verketteter Blöcke.

Adam Back empfahl im Mai 1997 Hashcash als Mechanismus, um den systematischen Missbrauch von nicht gemessenen Internet-Ressourcen wie E-Mail-Spams zu drosseln. Dieser Mechanismus basiert auf der Idee, dass jeder, der eine E-Mail verschickt, zuvor in eine Rechenleistung investieren und darüber einen Nachweis ablegen muss (Proof-of-Work). Nur wenn dies erfolgt ist, wird die Mail vom Empfänger akzeptiert. Die zu erbringende Rechenleistung ist beim Versenden einer Mail für den Absender kaum merkbar. Bei Massen- und Spam-Mails kann dieser Mechanismus jedoch unerwünschte Zeitverzögerung mit sich bringen. Auch wenn sich dieses Konzept für E-Mails nie so recht durchgesetzt hat, ist dieser Proof-of-Work beim Bitcoin wichtige Voraussetzung des sogenannten Minings, bei dem die Miner die Transaktion sowohl verifizieren als auch neue Coins schürfen [13] und diese in den Umlauf bringen.

Hashcoin verwendet ebenso wie die Blockchain kryptografische Hash-Funktionen,[14] Hashfunktionen wandeln eine Information beliebiger Länge in einen Hashwert[15] mit festgelegter Länge um (siehe z. B. Abb. 1).


Abb. 1: Umwandlung eines Textes in einen hexadezimalen Hashwert. [Katarina Adam 2019]

[11] Zwar erfüllt der Bitcoin alle Funktionen, jedoch ist er höchst volatil und damit ist die Aufbewahrungsfunktion eingeschränkt. Auch nehmen Händler diese Währung nur bedingt im Tausch gegen Waren an.
[12] Vgl. Back 2002.
[13] Beim Mining liegt die kryptografische Aufgabe darin, mit einer zweifachen SHA-256-Berechnung einen Hash-Wert zu finden, der unterhalb eines gewissen Grenzwertes liegt.
[14] Vgl. Güting / Dieker 2018, S. 128-129.
[15] Oft wird der Hashwert als eine hexadezimale Zeichenkette codiert, d.h. der Hashwert besteht aus einer Kombination aus Zahlen und Buchstaben zwischen 0 und 9 sowie A bis F (als Ersatz für die Zahlen 10 bis 15).

Die Hashfunktion SHA-256 (Secure Hash Algorithm 256) funktioniert nur in eine Richtung. Sie ist somit kollisionsfrei und das bedeutet, dass zwei verschiedene Inputwerte nicht auf denselben Outputwert kommen können. Gemäß dem obigen Beispiel ›*Es war ein großartiger Sonnenuntergang*‹ mit dem Hashwert

8e412b754db9d57983d22b2a4b0ef882a1798f7ef099f42bc576b162ef9d766b

kann nicht der gleiche Hashwert für den sinnverwandten Satz ›*Der Sonnenuntergang war großartig*‹ geschaffen werden. Im zweiten Falle lautete der Hashwert

fb15586a3ac8885b47582348996064954eea1b1fb6be62a35f1164ff6a5e686.

Dieses Prinzip ist die Grundlage des Proof-of-Work-Konzepts und wird in ähnlicher Form bei sämtlichen digitalen Währungen genutzt.

Eine weitere interessante Komponente bei der Ursprungs-Blockchain ist, wie Satoshi Nakamoto das sogenannte *Byzantine General Problem* für seine Anwendung genutzt hat. In der Informationstechnik wird mit dem *byzantinischen Problem* der Fehler beschrieben, bei dem sich ein System falsch bzw. völlig unerwartet verhalten kann.[16]

Das Problem beschreibt ein Szenario, in dem sich mehrere Generäle auf einen Zeitpunkt einigen müssen, an dem sie den gemeinsamen Feind angreifen wollen. Die Schwierigkeit dabei ist, dass einer oder mehrere der Generäle ein Verräter sein könnte, was in der Konsequenz bedeutet, dass er oder sie falsche Angaben über ihr Vorgehen machen könnten. Zum Beispiel könnte sich eine Gruppe von Generälen entschließen, eine Stadt anzugreifen und alle Generäle sind mit ihren Soldaten quasi sternförmig um die Stadtmauer verteilt. Von fünf Generälen sind zwei für Angriff und zwei für Rückzug. Der fünfte General sichert sowohl den Generälen, die für den Angriff stimmen, als auch den Generälen, die für den Rückzug sind, seine Unterstützung zu. Der Angriff scheitert, da dem Angriff kein Konsens des Handelns unterliegt.

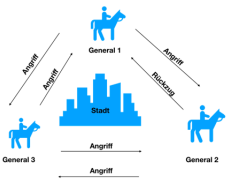


Abb. 2: Byzantine Generals Problem. [Katarina Adam 2019.]

[16] Vgl. Erstmalig wurde dieses Problem 1975 von Akkoyunly et al. 1975 aufgeworfen, detailliert von Lamport et al. 1982 beschrieben.

Die angreifenden Kräfte können die Stadt nicht erobern, weil keine zentrale Instanz das Vorhandensein von Vertrauen unter allen Generälen überprüfen kann. In diesem Szenario kann die sogenannte byzantinische Fehlertoleranz[17] dann erreicht werden, wenn die loyalen Generäle effektiv miteinander kommunizieren können, um die unbestrittene Einigung über ihre gemeinsame Strategie zu erzielen.

In der Bitcoin-Blockchain ist diese byzantinische Fehlertoleranz implementiert und das Problem wird über das Peer-to-Peer-Netzwerk (p2p) und ein Ledgersystem gelöst. Ein Algorithmus legt fest, welcher Miner den nächsten Block bestimmt und damit einigt sich das Netzwerk auf eine gemeinsame Wahrheit, die für und gegen jede*n Teilnehmer*in im Netzwerk gilt. Die Teilnehmenden an einem Netzwerk müssen sich nicht vertrauen, da alle Transaktionen transparent und nachvollziehbar sind. Dieses p2p-Netzwerk zeichnet Transaktionen nicht nur auf, sondern verifiziert diese. Ist die Mehrheit der Teilnehmenden des Netzwerkes der Ansicht, dass diese Transaktion korrekt ist, dann wird diese im Block gespeichert. Fehlerhafte Transaktionen werden identifiziert und entsprechend nicht weiter bearbeitet. Da sämtliche geprüfte und in den Blöcken gespeicherte Transaktionen nicht mehr veränderbar sind, ohne das dies auffällt (siehe veränderter Hashwert), wird Verlässlichkeit in die Transaktion gebracht. Es bedarf keines Mittelmanns mehr, der durch seine Position dafür bürgt, dass die durchgeführte Transaktion korrekt ist; das Netzwerk übernimmt diese Aufgabe.

Die Blockchain ist in erster Linie ein Aufzeichnungs-Ledger, der allen Beteiligten eine sichere und synchronisierte Aufzeichnung der Transaktionen von Anfang bis Ende bietet. Eine Blockchain kann Hunderte von Transaktionen sehr schnell aufzeichnen und nutzt hierfür mehrere kryptographische Mechanismen, um Datensicherheit zu gewährleisten.

Ähnliche Transaktionen auf der Blockchain werden zu einer funktionalen Einheit, einem Block, zusammengefasst und dann mit einem Zeitstempel (einem kryptographischen Fingerabdruck) versiegelt. Es können Daten nur in Blöcken angehängt werden, nicht jedoch wie bei herkömmlichen Datenbanken verändert oder gelöscht werden.

Die Bitcoin-Blockchain ist geschaffen worden, um Finanztransaktionen ohne Intermediäre direkt, schnell und zuverlässig abzuwickeln. Blockchains aber können viel mehr und dienen als Katalysatoren. Sie werden die Art und Weise, wie wir heutzutage Prozesse abwickeln, verändern und dies wird sich auf Regierung, Lebensweise, traditionelle Unternehmensmodelle, Gesellschaft und globale Institutionen auswirken.

[17]Die byzantinische Fehlertoleranz ist jenes Merkmal, das ein System definiert, welches die Klasse der Fehler toleriert, die zum Problem der byzantinischen Generäle gehören.

# 4. Blockchains der Generation 2.0

Mit der Bitcoin-Blockchain ist es möglich, finanzielle Transaktionen digital, schnell und direkt abzuwickeln. Jedoch ist es schwer, mit dieser Blockchain andere Werte zu transferieren. Dazu ist die Bitcoin-Blockchain über einen sogenannten Fork (Abzweigung) in die Ethereum-Blockchain durch u. a. Vitalik Buterin erweitert worden.

Ethereum nutzt die Grundlagen der Bitcoin-Blockchain, indem hier ebenfalls ein dezentrales Netzwerk agiert, jedoch ist Ethereum eine Plattform für sogenannte Distributed Apps (Dapps) und Distributed decentralized Organisation (DAO), die jeder Entwickler, jedes Unternehmen und / oder jede Privatperson auf der Plattform entwickeln und betreiben kann. Verteilte Knotenpunkte des Netzwerkes führen sogenannte Smart Contracts aus. Ein Smart Contract (kluger Vertrag) ist zunächst *nur* eine bindende Wenn-Dann-Abfolge. Es handelt sich hierbei um Programme, die auf einem Ledger / einer Blockchain abgelegt werden und deren Variablen-Werte durch Transaktionen geändert werden können. Smart Contracts sind jedoch nicht in der Lage, selbständig Transaktionen auszulösen. Vielmehr muss ein Benutzer-Account dieses initiieren.[18]

Mit dieser Erweiterung, nicht nur finanzielle Transaktionen über ein dezentrales Netzwerk abzubilden und abzuwickeln, ergeben sich neue Anwendungsmöglichkeiten. Zentral organisierte Systeme sind immer der Gefahr einer Attacke, eines Angriffs im Sinne einer Manipulation ihrer Daten ausgesetzt. Dezentralisierte Blockchain-Systeme hingegen legen dieses unmittelbar offen und sind in der Lage, entsprechend zu reagieren (beispielsweise, in dem die Transaktion als nicht valide in der Bearbeitung ignoriert wird).

Als vorteilhaft wird dabei angesehen, dass menschliches Versagen ausgeschlossen werden kann Anwälte nicht mehr zwingend für eine Vielzahl von Verträgen benötigt werden dieses zu Kosten- und Zeiteinsparungen führt die Verträge automatisch ausgeführt werden.

Nachteilig ist – zumindest aus juristischer Sicht – die Frage, wie eine Willenserklärung in einen Code gepackt werden kann. Eine Vielzahl an Jurist*innen beschäftigt sich daher sehr intensiv mit Fragestellungen dieser Art, um Smart Contract und das intrinsische Potential im juristischen Sinne zu kanalisieren.

Neben der erweiterten Nutzungs- / Anwendungsmöglichkeit können auf der Ethereum-Plattform ca. 15 Transaktionen pro Sekunde (TPS) durchgeführt werden. Auf der Bitcoin-Blockchain sind es dagegen nur ca. vier bis sieben Transaktionen pro Sekunde (TPS).

Auch wenn die Ethereum-Blockchain mehr als eine Verdopplung der Transaktionenabwicklungen pro Sekunde ermöglicht, reicht es nicht, um den Anforderungen der Realwirtschaft gerecht zu werden. Ziel sind bis zu einer Million TPS – und die Generation 3.0 arbeitet an entsprechenden Lösungen.

[18] Vgl. Ethereum.

## 5. Blockchains der Generation 3.0

Die Wirkungsweise von Blockchain-Lösungen und das große Veränderungspotential sind mittlerweile unbestritten. Was fehlt, ist der Übertrag in reale Prozessanforderungen und Prozessgeschwindigkeiten.

Weltweit arbeiten eine Vielzahl von Teams / Startups an Lösungen, um die TPS massiv zu erhöhen. Vitalik Buterin hat beispielsweise im Sommer 2018 bekräftigt, auch für die Ethereum-Plattform das Problem der Skalierbarkeit und der Netzwerküberlastung beheben zu wollen.[19]

Insgesamt geht es den auf dem Markt sichtbaren Lösungsansätzen im Prinzip darum, dass nicht alle Teilnehmer*innen des Netzwerkes jede Transaktion verifizieren müssen, sondern dass über Side-Chains oder Off-Chains verschiedene Transaktionen des Netzwerkes bearbeitet werden. Dieses *Ausgliedern* ermöglicht eine höhere Transaktionsgeschwindigkeit.[20] Viele Ansätze sind denkbar und fördern einen interdisziplinären Austausch, u. a. mit der Graphentechnologie.

## 6. Graphen

Netzwerke umgeben uns – nicht nur in der digitalen Welt. Beziehungen zu Familienmitgliedern, Freund*innen, Verwandten und Kolleg*innen sind ein solches (soziales) Netzwerk. In der IT existieren ebenfalls Netzwerke, gebildet aus Computern, Programmen und User*innen. Genau wie in der analogen Welt werden in der digitalen Welt Informationen ausgetauscht. Die Art des Austausches kann zentral oder dezentral organisiert sein. Die Beziehungen, die zwischen den Daten und Informationen bestehen, sind von Interesse und aus dem *richtigen* Herausfiltern der relevanten Informationen lassen sich Geschäftsmodelle kreieren.

Ein Graph stellt Objekte wie beispielsweise Knoten und Beziehungspunkte als Kanten dar und man unterscheidet sogenannte gerichtete (Darstellung einer Beziehung) und ungerichtete (symmetrische Beziehung) Graphen.[21]

»Graphdatenbanken sind dafür prädestiniert, relevante Informationsnetzwerke transaktional zu speichern und besonders schnell und effizient abzufragen. Das Datenmodell besteht aus Knoten, die mittels gerichteter, getypter Verbindungen miteinander verknüpft sind. Beide können beliebige Mengen von Attribut-Wert-Paaren (Properties) enthalten. Daher wird dieses Datenmodell auch als „ *Property-Graph* “ bezeichnet.«[22]

[19] Bei Ethereum werden das Sharding und Plasma als Möglichkeit genannt: Das Sharding erlaubt eine parallele Nutzung der Blockchain. Plasma wiederum verdichtet den Zugriff auf die Blockchain durch die Bündelung von vielen Transaktionen.
[20] Vgl. z. B. plasma, zk systems, constellation.
[21] Vgl. Güting / Dieker 2018, S. 201 ff.
[22] Vgl. Hunger 2014, S. 10.

Graphdatenbanken erzielen dank agilerer und flexiblerer Modelle vielfach eine bessere Performanz als herkömmliche, relationale Datenbanken, denn sie unterstützen systembedingt Datenstrukturen ohne sonst übliche Beschränkungen. Zusätzlich können Graphendatenbanken problemlos erweitert werden, ohne das bestehende Applikationen darunter leiden. Sie sind heute bereits häufig im Einsatz bei sozialen Netzwerken, Netz- und Cloudmanagement und auch bei der Betrugserkennung. Die Fähigkeiten von Graphdatenbanken sind daher auch für Blockchain-Entwickler*innen von hohem Interesse.

## 7. Blockchain vs. Graphdatenbank

Wie erläutert, ist die Blockchain eine Verkettung von Blöcken, die die getätigten und verifizierten Transaktionen enthalten. Diese Blöcke sind in ihrer Größe beschränkt (z. B. ermöglicht die Bitcoin-Blockchain maximal ein Megabyte) und damit auch in der Anzahl der Transaktionen. Weiterhin können nur Miner diese Blöcke erzeugen, was Kritiker*innen veranlasst, dieses als Machtvakuum anzusehen.

Graphen könnten eine Alternative sein, da sie diese Limitationen aufbrechen. Ledger können graphenbasiert organisiert werden. Jede*r Teilnehmer*in müsste dann schon im Netz vorhandene Transaktionen bestätigen, wenn er oder sie selbst eine Transaktion hinzufügen möchte. Blöcke wie bei der Blockchain sind dann nicht mehr nötig, sondern die Kanten des Graphen bilden die Transaktionsbestätigungen ab. Diese Transaktionsbestätigungen könnten sich anders verhalten als die bei der Blockchain. Ein graphenbasiertes Netzwerk ist ebenfalls dezentralisiert, jedoch existieren keine Rollen für das Erzeugen von Knoten.

Plattformen wie IOTA[23] oder Byteball[24] nutzen bei ihren Blockchain-Ansätzen dieses System der Graphen. Jedoch ist noch nicht sichergestellt, ob und wie dieses System sich verhält, welche Parameter benötigt und wie genutzt werden müssen, um ein stabiles und effektives Netzwerk zu haben.

Das Zusammenführen von Blockchain-Datenbanken und Graphdatenbanken ist ein vielversprechender Ansatz, um die großen Datenmengen von Heute und die der Zukunft so zu managen, dass sie die Vorteile beider Systeme vereinen und damit dezentrale, schnelle, transparente und effiziente Transaktionen ermöglichen. Aus Autorinnensicht ist es daher kein Blockchain versus Graphdatenbank, sondern vielmehr ein Miteinander.

[23] Vgl. IOTA.
[24] Vgl. Byteball White Paper Churyumov 2016, S. 4 ff.

# 8. Fazit / Herausforderungen

In der digitalen Ökonomie spielen Daten eine Schlüsselrolle. Wie sie gesichert, geschützt, aufbewahrt und genutzt werden, ist für den und die Einzelne*n von ebenso großer Bedeutung wie für Unternehmen. Jedoch ist die schiere Masse von Daten, die im Zuge der immer weiter fortschreitenden Digitalisierung produziert werden, nicht der eigentliche Wert. Der eigentliche Wert erschließt sich aus den Verknüpfungen von Daten.

Beide Datenbankenarten haben ihre Existenzberechtigung und wie immer gilt es zu prüfen, für welchen Anwendungszweck welches Instrument, welche Datenbank benötigt wird. Das Verschmelzen von Graphdatenbanken mit dem Ansatz der Blockchain-Technologie scheint sehr vielversprechend, denn viele ungelöste Fragen und Beschränkungen innerhalb der Blockchain-Technologie können, ergänzt um den Umgang mit Daten aus der Graphendatenbank, neu durchdacht werden.

Ein großes Problem und daher auch der Grund, warum noch keine massentaugliche Anwendung, die auf der Blockchain-Technologie basiert, aus dem Beta-Testing-Modus heraus ist, ist die Skalierbarkeit. Solange nur bis zu 15 TPS abgewickelt werden können, reicht dieses nicht aus, um in der Realwirtschaft zu bestehen. Auch, dass die gesamte Historie herunterzuladen ist, entwickelt sich bei Fortschreibung der Transaktion zu einem Hindernis. Die Bitcoin-Blockchain weist eine Größe von 179 MB auf (Stand Mitte August 2018) und allein diese Historie herunterzuladen dauert geschätzte 24 Stunden und mehr (je nach CPU). Ein weiteres, aber lösbares Hindernis ist die Interoperabilität zwischen sowohl den verschiedenen Blockchain-Arten als auch zu den klassischen (z. B.) Zahlungssystemen. Die neue Datenschutzgrundverordnung (DSGVO), die im Mai 2018 endgültig in Kraft getreten ist, stellt die Welt der Blockchains ebenfalls vor neue Herausforderungen.

Auch wenn es die (Bitcoin-)Blockchain seit gut zehn Jahren gibt, so sind noch viele Fragen unbeantwortet. Behördliche Fragen stehen ebenso im Raum wie rechtliche. Auf den ersten Blick vermag es so zu sein, dass die technischen Probleme leichter zu lösen sind, aber schon in dieser kurzen Zusammenfassung ist festzustellen, dass auch in diesem Zusammenhang noch viel Forschungs- und Entdeckungspotential vorhanden ist.

Daher, zum Vergleich: Es hat gut 20 Jahre gedauert, ehe das HTML-Protokoll das Internet-Protokoll ergänzte. Jedoch erst mit der Einführung des HTML-Protokolls schossen die Anwendungsmöglichkeiten in die Höhe und das World Wide Web wurde überhaupt erst möglich. In Bezug auf die Blockchain-Technologie stehen wir vor diesem Durchbruch. Jedoch vermag keiner zu sagen, wann er in welcher Form kommt. Sicher ist aber, der Durchbruch wird kommen!

# Bibliographische Angaben

Katarina Adam: Build to last: Blockchain on the cutting edge of the real. In: Industrie von morgen. Hg. von Matthias Knaut. Berlin 2017, S. 74–82. [Nachweis im GBV]

Eralp Abdurrahim Akkoyunly / Kattamuri Ekanadham / R. V. Huber: Some Constraints and Tradeoffs in the Design of Network Communikation. In: Proceedings of the fifth ACM symposium on Operating systems principles. (SOSP: 75, Austin, TX, 19.–21.11.1975) New York, NY 1975, pp. 67–74. [Nachweis im GBV]

Anonymus: How DigiCash Blew Everything. Hg. von Ian Grigg. In: cryptome.org. Beitrag vom 10.02.1999. [online]

Adam Back: Hashcash – A Denial of Service Counter Measure. 2002. PDF. [online]

Michael Bloss / Dietmar Ernst / Joachim Häcker / Nadine Eil: Von der Subprime-Krise zur Finanzkrise. München 2009. [Nachweis im GBV]

Usman Waqqas Chohan: The Double-Spending Problem and Cryptocurrencies, Discussion Paper. In: SSRN Electronic Journal (2017). Artikel vom 19.12.2017. DOI: 10.2139/ssrn.3090174

Anton Churyumov: Byteball: A Decentralised System for Storage and Transfer of Value. 2016. PDF. [online]

Henning Diedrich: Ethereum. Blockchains, digital assets, smart contracts, decentralized autonomous organizations. Lexington, KY 2016. [Nachweis im GBV]

Introduction to Smart Contracts. Hg. von Ethereum. Version v0.4.24. In: solidity.readthedocs.io. 2016–2018. [online]

Ralf Hartmut Güting / Stefan Dieker: Datenstrukturen und Algorithmen. 4., erweiterte und überarbeitete Auflage. Wiesbaden 2018. [Nachweis im GBV]

Michael Hunger: Neo4j 2.0. Eine Graphendatenbank für alle. Frankfurt / Main 2014. [Nachweis im GBV]

What is IOTA? A permissionless distributed ledger for a new economy. Hg. von IOTA Foundation. In: iota.org. Berlin 2018. [online]

Leslie Lamport / Robert Shostak / Marshall Pease: The Byzantine Generals Problem. In: ACM Transactions on programming languages and systems 4 (1982), no. 3, pp. 382–401. [Nachweis im GBV]

Sebastian Mallaby: The Man Who Knew. The Life & Times of Alan Greenspan. London u. a. 2016. [Nachweis im GBV]

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. PDF. [online]

Hans-Werner Sinn: Kasino-Kapitalismus. Wie es zur Finanzkrise kam. Berlin 2010. [Nachweis im GBV]

Nick Szabo: Bit Gold. In: nakamotoinstitute.org. Hg. von Satoshi Nakamoto Institute. Beitrag vom 29.12.2005. [online]

# Abbildungslegenden und -nachweise

Abb. 1: Umwandlung eines Textes in einen hexadezimalen Hashwert. [Katarina Adam 2019.]

Abb. 2: Byzantine Generals Problem. [Katarina Adam 2019.]