

Vorstellung der
Blockchain-Technologie
„Hallo, Welt!“



Einleitung

Die Entwicklung der Blockchain-Technologie verändert die Rolle traditioneller Player im Bereich Finance und Accounting grundlegend. Heute sind Transaktionen nur durch die besondere Vertrauensstellung von Banken und anderen Finanzdienstleistern möglich. In Zukunft kann die Blockchain diese Rolle übernehmen. Auch außerhalb des Finanzsektors entwickeln innovationsstarke Unternehmen neue Anwendungen auf Basis dieser Infrastruktur. Dieses Whitepaper stellt die Blockchain vor, zeigt Anwendungsmöglichkeiten auf und skizziert die mögliche Entwicklung dieser Technologie über die nächsten Jahre.

Die Geburtsstunde der Blockchain

Die Ursprünge der Blockchain liegen in der Kryptowährung Bitcoin. Im November 2008 publizierte eine unbekannte Person unter dem Pseudonym Satoshi Nakamoto ein technisches Konzept für digitales Bargeld unter dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“¹. Zu Beginn nutzten vor allem Kryptographie-Experten Bitcoins als Währung, heute genießen Bitcoins in weiten Kreisen dasselbe Vertrauen wie eine staatliche Währung.

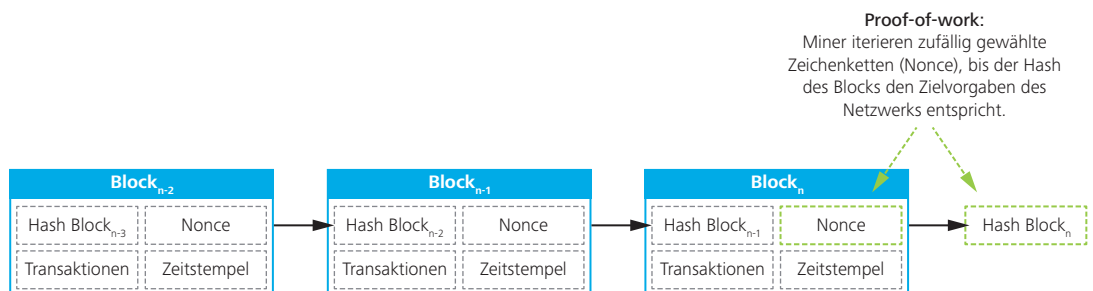
Nakamoto war keineswegs der Erste, der sich an der Erschaffung digitalen Geldes erprobte. Doch waren die Versuche seiner Vorgänger daran gescheitert, dass eine zentrale Autorität alle Transaktionen im Währungsraum überwachen musste, um die Gefahr des sog. Double Spending zu unterbinden. Nakamoto fand einen neuen Weg, das Double Spending zu verhindern: die Blockchain.

Double Spending ist das geteilte Schicksal aller digitalen Informationsgüter, seien es Währungseinheiten oder urheberrechtlich geschützte Werke: Sie sind nicht rivalisierend. Im Gegensatz zur Welt der körperlichen Gegenstände können digitale Güter unbegrenzt vervielfältigt werden. Dadurch ist es möglich sie zu nutzen, ohne dabei die Nutzungsmöglichkeiten anderer einzuschränken, getreu dem Motto „alles ist eine Kopie“. Ein funktionierendes Währungssystem ist darauf angewiesen, dass seinen internen Werteinheiten exklusive Nutzungsrechte zugeordnet werden können.

Funktionsweise der Blockchain

Die Blockchain selbst ist eine Datenbank, in welcher alle Bitcoin-Transaktionen verzeichnet werden. Im Rahmen des Validierungsverfahrens für Transaktionen („Mining“) werden Transaktionen in Blöcken zusammengefasst. Jeder Block verweist auf den ihm vorangegangenen gültigen Block, wodurch eine Kette, die „block chain“ entsteht. Einige Netzwerkteilnehmer, die sogenannten „Miner“, wetteifern darum, neue Transaktionsblöcke zu erstellen. Denn der erste Miner, der einen neuen Block findet, erhält eine Belohnung in Form neuer Bitcoins. Um einen Block zu finden, muss ein rechenintensiver Proof-of-work erbracht werden.

Abb. 1 – Der Aufbau der Blockchain: Jeder Block enthält einen Verweis von seinem Vorgängerblock



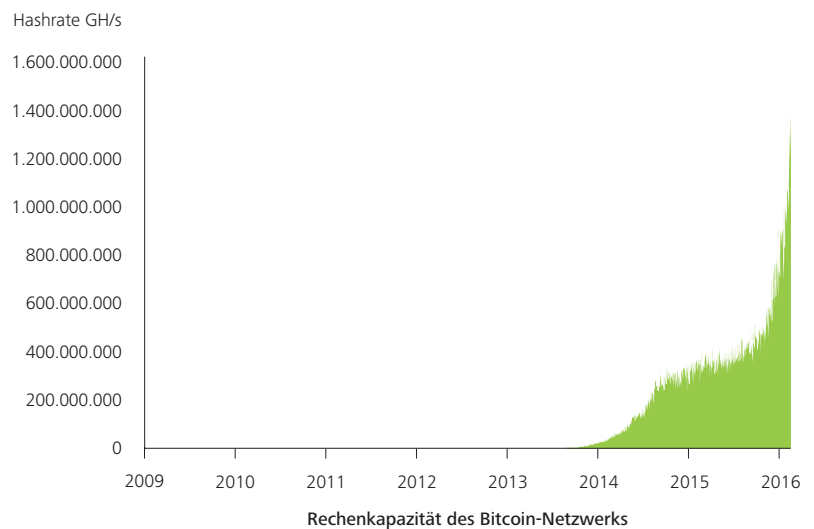
¹ <https://bitcoin.org/bitcoin.pdf>

Beim Proof-of-work-Verfahren geht es darum, wartende Transaktionen in einem neuen Block zu sammeln und den neuen Block an die Blockchain anzuhängen. Jeder Block enthält neben den gesammelten Transaktionen noch den Hash-Wert des Vorgängerblocks (Verkettung der Blöcke), einen Zeitstempel und eine Nonce (eine zufällig gewählte Zeichenkette).

Miner iterieren die Nonce und bilden nach jeder Iteration den Hash-Wert des neuen Blocks. Der Hash-Wert wird mit einem vom Netzwerk vorgegebenen Schwellenwert² verglichen (Difficulty). Wenn der Hash-Wert kleiner als der Schwellenwert ist, dann ist ein Block gültig und wird an die Blockchain angehängt. Der Miner, der den neuen Block gefunden hat, erhält dafür eine Belohnung in Form neu geschaffener Bitcoins.

Aufgrund der enorm hohen Rechenkapazität des gesamten Netzwerks gilt die Blockchain als praktisch fälschungssicher. Um einzelne Transaktionen in der Blockchain nachträglich zu verändern, müsste der Proof-of-work für die nachfolgenden Blöcke neu erbracht werden. Zusätzlich müssten die restlichen Teilnehmer die nachträglich geänderte Blockchain akzeptieren.

Abb. 2 – Die Entwicklung der Rechenkapazität im Blockchain-Netzwerk von 2009 bis heute
 Sie übersteigt die zusammengerechnete Kapazität der 500 schnellsten Supercomputer um ein Vielfaches.



Im Gegensatz zu herkömmlichen Datenbanken wird die Blockchain nicht auf einem einzelnen Computer (Server) vorgehalten. Alle Teilnehmer des Netzwerks („full nodes“) besitzen eine vollständige Kopie der kompletten Blockchain in ihrem lokalen Speicher. Man spricht deshalb von einer replizierten, geteilten Datenbank. Diese Eigenschaft ermöglicht es allen Netzwerkteilnehmern, Transaktionen lokal, d.h. für sich selbst zu validieren, ohne sich auf eine externe Aufsichtsinstanz verlassen zu müssen.

Abb. 3 – Modell verschiedener Netzwerktopologien

Die heutige Finanzwelt entspricht dem Modell links. Die Blockchain entspricht der Netzwerktopologie rechts.



² Der Schwellenwert wird an die Rechenkapazität des Netzwerks angepasst, sodass im Schnitt alle zehn Minuten ein neuer Block gefunden wird.

Die verteilte Natur der Blockchain stellt die Netzwerkteilnehmer vor die Herausforderung, stets eine gemeinsame Datengrundlage zu schaffen. Dazu wird ein Konsensalgorithmus verwendet. In der Blockchain einigen sich die Netzwerkteilnehmer immer auf die längste verfügbare Block-Kette.

Wem gehört die Blockchain?

Die Blockchain-Technologie ist „open source“.³ Bestehende Urheberrechte wurden an die Allgemeinheit abgetreten.⁴ Es gibt allerdings mehrere Parteien, welche die Weichen für die zukünftige Entwicklung dieser Technologie stellen.

Auf einer ganz grundsätzlichen Ebene sind es die „Miner“, also die Netzwerkteilnehmer. Sie validieren alle eingehenden Transaktionen. Dadurch sind sie eine Art Betreiber der verteilten Software-Plattform und können de facto über die konkrete Art des Betriebs entscheiden. Denn nur durch ihre Dienstleistung wird ein sicherer Geldverkehr ermöglicht. Entscheiden sie sich mehrheitlich, eine bestimmte Transaktion abzulehnen, d.h. diese nicht in validierte Blöcke miteinzubeziehen, so verändert sich dadurch letztlich die Funktionsweise der Blockchain selbst.

Tatsächlich benutzen die meisten Miner aber dieselbe Software zum Validieren eingehender Transaktionen, die sog. „bitcoind“-Standardimplementierung. Diese geht auf den Erfinder Satoshi Nakamoto selbst zurück. Diese weitverbreitete Software wird seitdem jedoch stetig weiterentwickelt. Das geschieht dabei in dezentralen Teams. Diese erarbeiten jeweils neue Verbesserungs- und Erweiterungsvorschläge der „bitcoind“-Software. Zusammen mit den anderen Teams wird letztlich über die Einbindung abgestimmt (sog. „Bitcoin Improvement Proposal“⁵). Mithin liegt also auch bei den Entwicklern dieser Software eine signifikante Entscheidungsmacht darüber, wie die Blockchain-Technologie ausgestaltet ist.

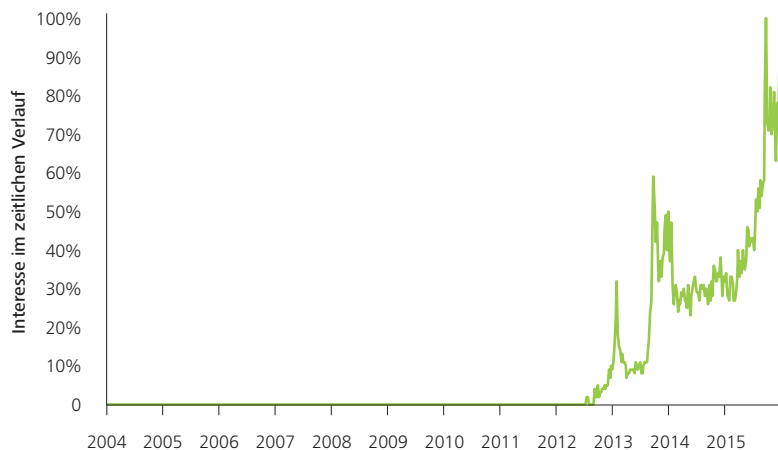
Daneben gibt es eine wachsende Zahl an Verbänden, die versuchen, auf die zukünftige Entwicklung der Blockchain Einfluss zu nehmen.⁶ Zunehmend gehören hierzu auch Dienstleister aus dem Bereich Accounting, welche das Potenzial der Technologie für sich erkannt haben.⁷

Blockchain

Nach den ersten Erfolgen des Bitcoin als neuartiger Währung verändert sich der Blick auf das Potenzial der darunterliegenden Blockchain-Technologie. Es ist klar, dass die Bedeutung geteilter, replizierter Datenbanken weit über die Erscheinung digitalen Bargelds hinausgeht. In der Blockchain können darüber hinaus auch andere Daten gespeichert und deren Integrität garantiert werden.⁸

Abb. 4 – Google-Trends für „Blockchain“:

Das Interesse an Blockchain-Technologie wächst rasant, eine immer größere Zahl an Unternehmen evaluiert den möglichen Einsatz von Blockchain-Technologie.



³ <https://github.com/bitcoin/bitcoin>

⁴ <https://github.com/bitcoin/bitcoin/blob/master/COPYING>

⁵ <https://github.com/bitcoin/bips>

⁶ Vgl. www.bundesverband-bitcoin.de und www.bitcoinfoundation.org

⁷ <http://www.ibtimes.co.uk/deloitte-libra-accenture-work-auditors-age-bitcoin-2-0-technology-1515932>

⁸ Seit dem Jahr 2013 investieren die Risikokapitalgeber des Silicon Valley dreistellige Millionenbeträge in Startups, die mit Blockchain-Technologie arbeiten.

⁹ Google Trends ist ein normierter Index, der die Popularität eines Suchbegriffs im Zeitverlauf darstellen soll. Desto höher der Wert, desto höher die Popularität des Suchbegriffs, relativ zu vorherigen Suchanfragen über die Zeit.

Damit ergibt sich großes Potenzial für innovative Produkte und Services, die Prozesse im öffentlichen und privatwirtschaftlichen Bereich vereinfachen können. Überall da, wo die nachweisliche Integrität von Daten eine Rolle spielt, kann die Blockchain-Technologie für Wandel sorgen. Nicht nur Startups arbeiten an neuen Services nach dieser Logik, mittlerweile planen auch viele Unternehmen und Staaten, die Technologie einzusetzen:

Neben den genannten Möglichkeiten erstrecken sich die Anwendungen auf zahlreiche weitere Bereiche des Wirtschaftslebens.



Im Oktober 2014 wurde die erste Heirat in der Blockchain notariell beurkundet, gleich einer Eintragung in einem behördlich geführten Personenstandsregister.¹⁰



Die Universität Nicosia zertifiziert die Zeugnisse ihrer Studenten in Form von Transaktionen in der Blockchain.¹¹



Die britische Regierung erforscht den Nutzen der Integritätsgarantie der Blockchain.¹²



Die Isle of Man betreibt ein Handelsregister für Unternehmen im Kryptowährungsbereich basierend auf der Blockchain.¹³



In der Initiative R3 haben sich 30 weltweit agierende Banken zusammengefunden, um eine eigene, private Blockchain zu entwickeln, mit der Zahlungen kostengünstig abgewickelt werden können. Diese Art von Blockchain wird auch als „Permissioned Ledger“ bezeichnet.¹⁴



Deloitte arbeitet mit Blockchain-Technologie, um größeres Vertrauen in die Bücher von Firmen zu schaffen und Prüfungen zu automatisieren.¹⁵



IBM wagt im Jahr 2015 mit seiner ADEPT-Initiative einen neuen Vorstoß, um die weltweite IoT-Infrastruktur auf ein Blockchain-basiertes System umzustellen.¹⁶

Ausblick

Die Blockchain-Technologie steht noch am Anfang. Das riesige Potenzial wird von vielen unterschiedlichen Marktteilnehmern – insbesondere aus der Finanzbranche – erprobt. Viele neue Anwendungen werden entwickelt, um bestehende Prozesse zu vereinfachen und zu automatisieren. Das Interesse an der Blockchain-Technologie ist ungebrochen – gleichzeitig erhöht sich aufgrund der vielen neuen Netzwerkteilnehmer die Fälschungssicherheit immer weiter.

Über die Autoren

Jannis Holthusen, Simon Kufeld und Florian Glatz sind die Gründer der Upchain GmbH. In Kooperation mit Deloitte entwickeln sie eine neue Datenplattform für aufbewahrungspflichtige Unterlagen auf Basis der Blockchain-Logik. Damit können Unternehmen die Integrität ihrer Daten nachweislich sicherstellen und Prüf- und Kontrollprozesse stärker automatisieren.

¹⁰ <http://bitcoinmagazine.com/17066/first-blockchain-wedding-2/>

¹¹ <http://digitalcurrency.unic.ac.cy/certificates>

¹² https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/g5-16-1-distributed-ledger-technology.pdf

¹³ <http://www.coindesk.com/isle-of-man-trials-first-government-run-blockchain-project/>

¹⁴ <https://www.linkedin.com/company/r3cev-llc>

¹⁵ www.ibtimes.co.uk/deloitte-delving-into-ethereum-eris-ripple-1515494

¹⁶ <http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings>

Ihr Ansprechpartner

Nicolai Andersen

Partner, Leiter Innovation
Deloitte Deutschland
Tel: +49 (0)40 32080 4837
nicandersen@deloitte.de

Für weitere Informationen besuchen Sie unsere Website www.deloitte.com/de/blockchain

Die Deloitte Consulting GmbH („Deloitte“) als verantwortliche Stelle i.S.d. BDSG und, soweit gesetzlich zulässig, die mit ihr verbundenen Unternehmen und ihre Rechtsberatungspraxis (Raupach & Wollert-Elmendorff Rechtsanwaltsgesellschaft mbH) nutzen Ihre Daten im Rahmen individueller Vertragsbeziehungen sowie für eigene Marketingzwecke. Sie können der Verwendung Ihrer Daten für Marketingzwecke jederzeit durch entsprechende Mitteilung an Deloitte, Business Development, Kurfürstendamm 23, 10719 Berlin, oder kontakt@deloitte.de widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), eine „private company limited by guarantee“ (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global“ genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Steuerberatung, Corporate Finance und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für mehr als 225.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte Consulting GmbH noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk“) erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.