DIGITALES ARCHIV

ZBW – Leibniz-Informationszentrum Wirtschaft
ZBW – Leibniz Information Centre for Economics

Möbert, Jochen

Book

Die multiplen Stufen der Blockchain-Revolution : oder einmal Kryptohype und zurück

Provided in Cooperation with:
Deutsche Bank Research, Frankfurt am Main

Reference: Möbert, Jochen (2018). Die multiplen Stufen der Blockchain-Revolution : oder einmal Kryptohype und zurück. Frankfurt, Main : DB Research.

This Version is available at:
http://hdl.handle.net/11159/2826

Kontakt/Contact
ZBW – Leibniz-Informationszentrum Wirtschaft/Leibniz Information Centre for Economics
Düsternbrooker Weg 120
24105 Kiel (Germany)
E-Mail: *rights[at]zbw.eu*
https://www.zbw.eu/econis-archiv/

Standard-Nutzungsbedingungen:
Dieses Dokument darf zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden. Sie dürfen dieses Dokument nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen. Sofern für das Dokument eine Open-Content-Lizenz verwendet wurde, so gelten abweichend von diesen Nutzungsbedingungen die in der Lizenz gewährten Nutzungsrechte.

https://zbw.eu/econis-archiv/termsofuse

Terms of use:
This document may be saved and copied for your personal and scholarly purposes. You are not to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public. If the document is made available under a Creative Commons Licence you may exercise further usage rights as specified in the licence.

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Mitglied der Leibniz-Gemeinschaft

Deutsche Bank
Research

EU-Monitor

Digitale Ökonomie und struktureller Wandel

Die multiplen Stufen der Blockchain-Revolution

Oder einmal Kryptohype und zurück

22. November 2018

Autor
Jochen Möbert
+49 69 910-31727
jochen.moebert@db.com

Editor
Stefan Schneider

Deutsche Bank AG
Deutsche Bank Research
Frankfurt am Main
Deutschland
E-Mail: marketing.dbr@db.com
Fax: +49 69 910-31877

www.dbresearch.de

DB Research Management
Stefan Schneider

Seit dem Preisboom im Jahr 2017 sind die Schlagwörter Bitcoin und Blockchain in der Gesellschaft allgegenwärtig. Trotzdem ist das Verständnis vom Potenzial der Technologie oft rudimentär.

Um die Diskussion zu schärfen, diskutieren wir sowohl die vielen technologischen Facetten als auch die mit der Technologie möglicherweise einhergehenden gesellschaftlichen Veränderungen. Wir beschreiben zehn Stufen, die jede für sich eine kleine gesellschaftliche Revolution darstellt. Alle Stufen zusammen erklären, warum die Enthusiasten von der globalen Blockchain-Revolution träumen.

Nur zwei der zehn Stufen stellen dabei eine Revolution unseres Geldsystems dar. Denn die Kerninnovation einer Blockchain ist das Fixieren von Informationen. Somit erhält man eine verlässliche Datenbasis für deutlich mehr als nur Geld. Zum Beispiel könnten auf Blockchains Eigentumsrechte geregelt werden. Die Kommunikation zwischen Fahrzeugen, Maschinen und Robotern könnte ebenfalls über Blockchains erfolgen. Durch die Speicherung komplexer und codebasierter Wenn-Dann-Logik könnten schließlich auch Verträge fixiert und ausgeführt werden. Genauso wäre es theoretisch möglich, verlässliche Abstimmungen aller Art über Blockchains zu organisieren.

Nachdem wir die Utopie aufgezeigt haben, benennen wir die technischen, aber auch gesellschaftlichen Hindernisse, die der Revolution im Wege stehen. Eine rasante Umsetzung erwarten wir nicht. Vielmehr dürfte es noch viele Jahre, vielleicht sogar Jahrzehnte dauern, bis die neue Technologie eine hohe Marktdurchdringung erzielt und ganz selbstverständlich in unserem Alltag eingebunden ist.

1. Stufe: Ein außerstaatliches Zahlungsmittel

Eine Gruppe von libertären Computerexperten, die sich Cypherpunks nennen, entwickelt schon seit Jahrzehnten außerstaatliches Geld. Doch alle Versuche, solche alternativen Zahlungsmittel zu etablieren, scheiterten.

Eine Ursache für das Misslingen war die Zentralität der Systeme, denn wie viele Innovationen waren sie juristisch an die Existenz eines Unternehmens gekettet. Daher versagten viele dieser Bitcoin-Vorläufer nicht nur an der fehlenden Marktdurchdringung, sondern auch an Refinanzierungsrisiken und staatlichen Verboten. Die vielen negativen Erfahrungen der Cypherpunks vor dem Jahr 2009 flossen wohl in die Entwicklung von Bitcoin ein. Denn wenngleich die Identität hinter dem Pseudonym Satoshi Nakamoto weiterhin unbekannt ist, belegen viele Indizien die intellektuelle Nähe zu den Cypherpunks. Zweifellos hat auch Bitcoin als Zahlungsmittel bis heute eine niedrige Marktdurchdringung. Die maximale Zahl lag bei rund 1 Mio. Bitcoin-Transaktionen pro Woche, also 200.000 Transaktionen pro Tag. Wenn eine Person durchschnittlich zehn Transaktionen pro Tag auslöst, dann war das globale Zahlungsmittel Bitcoin immerhin in der Lage, eine 20.000 Einwohner große Kleinstadt zu versorgen. Neben diesen sogenannten on-chain Transaktionen ist seit Anfang des Jahres 2018 auch das Lightning Network live gegangen. Diese off-chain Transaktionen werden hauptsächlich für kleine alltägliche Einkäufe und Mikropayments verwendet. Standardbeispiele sind der Kauf eines Kaffees oder die sekundengenaue Abrechnung von Streamingdiensten, wie zum Beispiel beim Anschauen von Videos. Aktuelle Statistiken zeigen ein rasantes Wachstum der Knoten und Payment Channels im Lightning Netzwerk. Trotzdem liegt die monetäre Kapazität des Lightning Networks bei nur rund 100 Bitcoins, was bei aktuellen Marktkursen deutlich weniger als EUR 1 Mio. entspricht. Führt in unserer 20.000 Einwohner großen Kleinstadt jeder EUR 100 Bargeld für alltägliche Transaktionen mit sich, dann liegt der Bargeldumlauf dieser Stadt bei EUR 2 Mio. und damit mehr als doppelt so hoch wie die „Kaufkraft“ des Lightning Networks. Sowohl on-chain als auch off-chain ist das globale Zahlungsmittel Bitcoin also zumindest bis heute im besten Fall eine Nische[1].

November 2018: Kapazität des Lightning Networks 1

in Bitcoin

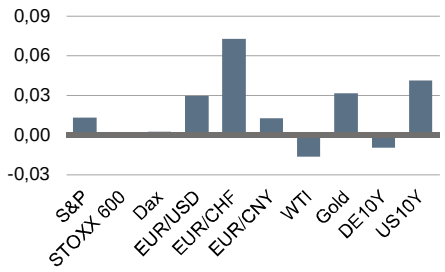
Quellen: 1ML, Deutsche Bank Research

2. Stufe: Ein schwer zu regulierendes Spekulationsobjekt

Tatsächlich dürfte Bitcoin als Zahlungsmittel, also Bitcoin gegen Ware oder Dienstleistung, noch unbedeutender sein, als wir es dargelegt haben. Denn Bitcoin ist vor allem ein Spekulationsobjekt und das erste Vehikel einer neuen Anlageklasse. Entsprechend wollen die Anleger ihre erhofften Gewinne später wieder in staatliches Geld tauschen, was sie auch teilweise müssen, z.B. um Steuern zu bezahlen. Die Kryptoinvestoren hoffen weiterhin auf hohe Renditen, die sich aus steigenden Nutzer- und Anlegerzahlen ergeben sollen. Tatsächlich stieg deren Zahl in der Vergangenheit mit dem Ausbau der Infrastruktur rund um die Kryptowährungen an. Zunächst erfolgte der Aufbau von Kryptobörsen, um Bitcoin gegen Euro und US-Dollar zu tauschen. Wenig später entstanden traditionelle Investitionsvehikel, wie geschlossene Fonds und ETNs (Exchange-Traded Notes), die Investitionen in den Kryptomarkt erlauben und zwar ganz ohne den Aufbau von Fachwissen. Im Jahr 2017 entstanden Futures-Märkte mit Cash-Settlement, d.h. Verluste aus den Futures-Positionen werden in US-Dollar beglichen. Für das Jahr 2019 plant die Intercontinental Exchange die Einfüh-

5jährige Korrelationen: Bitcoin vs. Finanzmarktindizes 2

[-1,+1]



Quellen: Deutsche Bank Research, IHS Global GmbH

[1] Möbert, Jochen (2018). Bitcoin: Meinungen, Mythen und Missverständnisse. EU-Monitor. Deutsche Bank Research.

rung von Futures-Märkten mit physischem Settlement, d.h. Verluste aus den Futures-Geschäften werden direkt in Kryptowährungen beglichen. Entsprechend haben viele Investoren die Hoffnung, dass bald eine Massenadaption erfolgt, beispielsweise wenn die US-Behörden ETFs erlauben oder auf andere Art und Weise Kryptowährungen als Anlageklasse bei den Family Offices und institutionellen Investoren Anerkennung finden. Neben der Hoffnung auf weitere Renditesprünge können Kryptowährungen auch als Absicherung gegen Finanzmarktrisiken dienen. Die hohen staatlichen und privaten Schulden in vielen Ländern dürften neue Krisen generieren, wodurch außerstaatliche Geldsysteme an Attraktivität gewinnen könnten. Aber auch außerhalb von Krisenzeiten weisen Kryptowährungen eine geringe Korrelation mit Aktien, Anleihen und Immobilien auf. Durch die Beimischung von Kryptowährungen könnten Portfolios ein besseres Risiko-Rendite-Verhältnis aufweisen. Jedoch dürfte aufgrund der hohen Volatilität von Kryptowährungen und aufgrund des hohen Risikos eines Totalausfalls der optimale Portfolioanteil bei vielen Kunden eher im (sehr) niedrigen einstelligen Prozentbereich liegen.

3. Stufe: Informationen zementieren

Die Blockchain ermöglicht es, ein funktionierendes, relativ langlebiges globales außerstaatliches Zahlungssystem und ein schwer zu regulierendes Spekulationsobjekt zu erschaffen. Da das ganze System zudem ohne zentrale Institution auskommt, zieht es einige Aufmerksamkeit auf sich – zumal diese Entwicklung historisch einzigartig ist. Aber das Innovationspotenzial der Technologie ist deutlich größer. Dies wird klar, wenn man Blockchain als Informationskette mit zwei wesentlichen Eigenschaften versteht:

- Erstens ist die gesamte Historie jeder Informationskette von ihrer Entstehung bis heute jederzeit abrufbar.
- Zweitens kann die Informationskette dank Kryptografie und tausender Kopien, die auf Rechnern in vielen Ländern gespeichert sind, nicht manipuliert werden. Mit einem solchen System kann man also Informationen „zementieren“ und folglich eine Vertrauensbasis schaffen.

Wenn Bitcoin nur eine digitale Information ist, wieso halten dann alle diese einzelne Information für einen Coin einer Währung? Die Antwort lautet: Nur deshalb, weil alle denken, dass alle glauben, dass die Information eine Währung ist. Die Währung entsteht folglich aus dem Nichts. Stellen Sie sich jetzt vor, eine Gesellschaft definiert eine Information nicht als Coin, sondern als Grundstück. Wenn alle denken, dass alle glauben, dass die Information einer Blockchain ein Grundstück repräsentiert, dann erfolgt der Eigentumstransfer eines Grundstücks ganz ohne Notare und vor allem ohne Notargebühren. Das klingt zweifellos utopisch. Doch es gibt eine Reihe von Ländern, die an Pilotprojekten arbeiten, um in einer wohl eher fernen Zukunft Eigentumsübertragungen von Grundstücken und Gebäuden auf einer Blockchain zu verwalten.

Wenn Informationen auf der Informationskette sowohl eine Kryptowährung als auch ein Grundstück repräsentieren können, welche Informationen können noch mit einer Blockchain verwaltet werden? Wenn Eigentumsübertragungen von Grundstücken möglich sind, dann dürften auch Aktien, Anleihen und Derivate auf der Blockchain handelbar sein. Gleiches gilt für staatliches Krypto-Geld, also Krypto-Euros oder Krypto-Dollar. Aber auch Copyright-Rechte an Liedern und Filmen, persönliche Gesundheitsdaten oder gleich komplette digitale Identitäten, wobei die Personen dank Kryptografie – im Gegensatz zum Status quo – die volle Kontrolle über ihre Daten behalten. Die Blockchain-Enthusiasten würden auf die Frage, welche Informationen noch mit einer Blockchain verwaltet werden

können, antworten: „alle!“. Folglich erwarten sie eine Revolution, die alle Informationen des Dienstleistungssektors auf die Blockchain hebt und potenziell alle zentralen Akteure, insbesondere in der Verwaltung und Überprüfung von Informationen, obsolet macht.

4. Stufe: Maschinenkommunikation über IT-Systeme hinweg

Doch die Blockchain-Revolution könnte nicht nur den Dienstleistungssektor auf den Kopf stellen, sondern ebenso das Verarbeitende Gewerbe. Maschinenkommunikation oder neudeutsch „Internet of Things“ (IoT[2]) findet heute vor allem innerhalb von Fabriken und damit innerhalb eines Unternehmens statt. Beispielsweise, wenn der eine Greifarm am Fertigungsband seinen „Roboterkollegen“ meldet: „Das ist mein Revier, wartet bis ich meine Arbeit erledigt habe.“ Innerhalb einer Fabrik und damit innerhalb einer zentral gesteuerten Hierarchie können diese Regeln einfach angeordnet werden. Kommunizieren Maschinen jedoch miteinander über verschiedene IT-Systeme und juristische Einheiten hinweg oder gleich im öffentlichen Raum, benötigt man eine digitale Vertrauensbasis. Die nicht manipulierbaren Blockchains könnten genau diese Basis darstellen, auf die sich die Maschinen bzw. ihre Programmierer verlassen. Folglich könnten beispielsweise die verschiedenen Autobauer gemeinsam einen Kommunikationsstandard etablieren, der ihr Auto sowie den gesamten Straßenverkehr über eine Blockchain steuert. Solche dezentralen Lösungen könnten auch einen digitalen Systemkollaps und dessen potenziell katastrophale Unfallfolgen verhindern oder diesen im Vergleich zu einer zentralen Lösung zumindest deutlich unwahrscheinlicher machen. Blockchains sind quasi prädestiniert zur Steuerung kritischer Infrastruktur, da sie dank dezentraler Informationsverteilung auch robuster gegenüber Cyberattacken sind als traditionelle IT-Systeme. Die Umsetzung dezentraler Lösungen im Straßenverkehr ist noch ferne Zukunftsmusik, wenngleich es auch hier erste Pilotprojekte gibt. Der Schienenverkehr könnte dagegen schon deutlich früher von Blockchain-Lösungen profitieren. Die Deutsche Bahn arbeitet intensiv daran, die mehrere hundert in Deutschland gemeldeten Bahnunternehmen über eine gemeinsame Blockchain zu steuern und praktisch in Echtzeit die Unternehmen für ihre erbrachten Dienstleistungen zu entlohnen.

5. Stufe: Smarte Verträge unwiderruflich festschreiben

Für eine flexible Handhabung einer komplexen Steuerung ist die Zementierung von Informationen hilfreich. Doch auf einer Blockchain können auch komplette und komplexe Wenn-Dann-Logiken abgelegt werden. Verträge können folglich von Programmieren in Code übersetzt und auf einer Blockchain unwiderruflich festgeschrieben werden. Im juristischen Sinne kommen diese sogenannten „Smart Contracts“ durch inhaltlich übereinstimmende Willenserklärungen zustande – also wie jeder andere Vertrag auch. Was wäre es für ein Fortschritt, wenn es eine Versicherung für Zugverspätungen gäbe, deren Vertrag auf einer Blockchain abgelegt würde und die im Versicherungsfall dank Smart-Contract-Lösung automatisch und unbürokratisch eine Entschädigung auszahlte. Für Flugverspätungen ist eine solche Blockchain-basierte Versicherung bereits implementiert. Eine intensive Nutzung von Smart Contracts könnte unseren Alltag in vielerlei Hinsicht verändern und vereinfachen.

[2] Auer, Josef (2018). Industrie 4.0 – Digitalisierung mildert demografische Lasten. Deutschland-Monitor. Deutsche Bank Research.

6. Stufe: Smart Contracts plus künstliche Intelligenz (KI)

Haben sich Smart Contracts erst einmal fest in unserem Alltag etabliert, liegt die nächste Revolution nur einen Steinwurf entfernt. Durch den Einsatz künstlicher Intelligenz könnte der Anwendungsbereich von Smart Contracts explodieren. So könnte ein mit Kameras und Sensoren vollgepacktes Unfallauto in Zukunft dank intelligenter Algorithmen einen Unfallhergang rekonstruieren. Aufwändige juristische Verfahren könnten so überflüssig werden. Die künstliche Intelligenz könnte nahezu zeitgleich mit dem Unfall den Krankenwagen rufen und noch vor dessen Eintreffen die Schadensregelungen einleiten. Die Geschädigten verfügten also sofort über die finanziellen Mittel, um Arztrechnungen zu bezahlen und den Arbeitsausfall auszugleichen.[3]

Zahlreiche weitere Alltagsbeispiele existieren. Die Pharmaindustrie, Krankenkassen und der Endverbraucher könnten deutlich effizienter miteinander kommunizieren und mehr voneinander profitieren als heute. Die Einnahme von Medikamenten könnte beispielsweise über Sensoren am Handgelenk mittels regelmäßiger Puls- und Blutdruckmessung oder auch im Sanitärbereich auf einer Blockchain erfasst werden. Krankenkassen könnten den Patienten für die verordnungsgemäße Einnahme belohnen. Gleichzeitig könnte dem Produzenten eine Vielzahl von Informationen gemeldet werden, beispielsweise die eingenommene Medikamentenmenge, Einnahmehäufigkeit, Uhrzeit und vieles mehr. Erfolgt die Auswertung dieser Daten mittels künstlicher Intelligenz könnte die künftige Einnahme der Medikamente durch die Berücksichtigung individueller Patientenmerkmale individualisiert und somit optimiert werden. Dabei garantiert die kryptografisch abgesicherte Speicherung dieser Informationen auf einer Blockchain die Einhaltung der Datenschutzbestimmungen. Der Patient gewährt beispielsweise seiner Krankenkasse lediglich Zugang zu der Information: Alle Medikamente wurden verordnungsgemäß eingenommen. Dem Pharmaproduzenten stellt der Patient dagegen die individuellen, aber anonymisierten Patientendaten gegen Bezahlung zur Verfügung. Auch die Rolle des Arztes könnte so neu definiert werden. Verläuft der Heilungsprozess wie erwartet, reduziert sich die Zahl der Arztbesuche. Bei unerwarteten Krankheitsverläufen könnte der Patient automatisch einen zusätzlichen Arzttermin angeboten bekommen. Folglich könnte die Vertrauensbasis Blockchain auch sensible Daten in kontrollierter Form der Gesellschaft zur Verfügung stellen. Viele weitere Kombinationen von Smart Contracts und künstlicher Intelligenz könnten bedeutende Bausteine der Blockchain-Zukunft sein.

7. Stufe: Die globale KI-Gesellschaft

Blockchains könnten zusammen mit künstlicher Intelligenz aber nicht nur im Alltag Anwendungen finden, sondern auch die Grenzen unserer Wissensgesellschaft verschieben. Viele komplexe wissenschaftliche Fragestellungen, zum Beispiel bei der Entwicklung neuer chemischer Stoffe oder der Berechnung von Klimamodellen erfordern die Auswertung großer Datenmengen. Diese Algorithmen könnten künftig zunehmend über global vernetzte Computer anstatt über zentrale Großrechner oder Supercomputer erfolgen. So kann eine ungeheure Rechenkapazität auf flexible Art und Weise vorgehalten, ausgelastet und weiterentwickelt werden. Gleichzeitig erlaubt dieser Ansatz eine hohe Spezialisierung einzelner Computer oder eines Teils des Netzwerkes auf spezifische KI-Algorithmen. Diese Spezialisierung kann einerseits die Effizienz des gesamten Netzwerkes erhöhen, andererseits können komplexe Berechnungen in Teilprob-

[3] Otto-Schleicher, Daniel und Florian Bauer (2018). Die wahren Treiber der Blockchain-Revolution. capital.de.

Tech Talk: Die Blockchain Revolution – Kryptowährungen, Video 1/3 5

Quelle: Deutsche Bank Research

leme zerlegt, von den spezialisierten Algorithmen berechnet und als Teillösungen dem Gesamtnetzwerk gemeldet werden. Die Blockchain-Technologie kann die Erschaffung und Fortentwicklung solcher globalen Computer- und Informationsnetzwerke massiv erleichtern. Eine Kryptowährung kann eine effiziente Allokation von Rechenproblemen auf die verschiedenen Algorithmen ermöglichen, folglich die dahinterstehenden Programmierer belohnen und Anreize setzen, das System stetig zu verbessern. Zudem können die durch die Algorithmen berechneten Teilergebnisse auf einer Blockchain gespeichert und so verlässlich dem globalen Computernetzwerk zur Verfügung gestellt werden. In diesem Kontext könnten Blockchains ein wesentlicher Baustein der zunehmenden Bedeutung von künstlicher Intelligenz für die Gesellschaft und Wirtschaft der Zukunft sein.

8. Stufe: Erhoffte Entpolitisierung durch Blockchains

Tech Talk: Die Blockchain Revolution – Gesellschaftliche Implikationen, Video 2/3 6

Quelle: Deutsche Bank Research

Eine weitere Entwicklungsstufe der Blockchain-Revolution ist die Vorstellung, dass eine völlig neue Gesellschafts- und Wirtschaftsordnung in der Zukunft möglich sein könnte. Dies ist keine zufällige Entwicklung. So war es von Anfang an ein Anliegen der Cypherpunks, alle menschlichen Beziehungen ganz ohne Dritte und ganz ohne zentrale – insbesondere staatliche – Institutionen zu ermöglichen. Sie träumten und träumen davon, die heute Vertrauen schaffenden Institutionen, in denen sich aus ihrer Sicht eine zu hohe Machtkonzentration bündele, durch unbestechliche, niemals korrupte und niemals politisch gefärbte Blockchain-Lösungen zu ersetzen.

9. Stufe: Digitale Demokratie ermöglichen

Diese Entpolitisierung der Gesellschaft könnte mittels Blockchains auch über mehr direkte Demokratie erfolgen. Wie wir oben beschrieben haben, können auf einer Blockchain Informationen zementiert werden, beispielsweise die Stimmabgabe bei einer Wahl.[4] Die Kryptografie garantiert dank Verschlüsselung die Einhaltung des Wahlgeheimnisses und dank individueller Entschlüsselung das jederzeitige nachträgliche Verifizieren der eigenen Stimmabgabe. Die Blockchain-Technologie könnte die Wahlkosten massiv senken und hat das Potenzial, sowohl die Wahl per Brief als auch im Wahllokal überflüssig zu machen. Doch bedeutender als das Einsparungspotenzial könnten die gesellschaftlichen Implikationen sein. In den demokratischen Ländern könnte die Forderung, die Bürger intensiver an politischen Entscheidungen zu beteiligen, mehr Gewicht erhalten. Theoretisch wäre eine direkte Demokratie vorstellbar, in der die Bürger regelmäßig abstimmen und die parlamentarischen Entscheidungen ergänzen oder gar teilweise ersetzen.

Tech Talk: Die Blockchain Revolution – Geschäftsideen und Lösungen für die Wirtschaft, Video 3/3 7

Quelle: Deutsche Bank Research

10. Stufe: Dezentrale autonome Organisationen (DAO)

Wenn viele Menschen effizient und nachvollziehbar ihre politische Stimme abgeben können, dann ist die nächste Revolution nicht fern. Blockchain-Lösungen machen die alte Redensart „Viele Köche verderben den Brei“ womöglich obsolet. Denn so wie Demokratien den Wählerwillen schnell und effizient

[4] So hat der US-Bundesstaat Maine im Frühjahr 2017 eine Kommission eingesetzt, um zu untersuchen, ob neben der klassischen Abstimmung mit Zettel und Stift parallel auch Wahlen auf der Blockchain abgehalten werden sollen. https://legislature.maine.gov/legis/bills/bills_128th/billtexts/SP030501.asp

über Blockchains erfassen könnten, so ließe sich auch zumindest die Entscheidungsfindung großer Organisationen steuern. Potenziell könnten Vereinsmitglieder gemeinsam über eine Blockchain ihren Verein leiten oder Eigentümer wesentliche Entscheidungen eines Unternehmens ohne Management treffen. Solche sogenannten DAO könnten unser Handeln und Wirtschaften neu definieren. Neben den klassischen hierarchischen Systemen, die unsere gesamte Gesellschaft seit jeher prägen, ist im Zuge der Blockchain-Revolution eine Etablierung dezentraler Entscheidungssysteme zumindest theoretisch vorstellbar.

Das war die Utopie. Nun ist es Zeit für eine kritische Einordnung: Die Blockchain-Revolution dürfte noch auf sich warten lassen!

Den Traum haben wir aufgezeigt und sind selbst von den heutigen und künftigen technischen Möglichkeiten durchaus begeistert. Doch es bestehen unserer Ansicht nach eine Reihe von Engpässen, welche die globale Blockchain-Revolution ausbremsen: Blockchains

(1) sind sehr teuer,

(2) können von nur wenigen entwickelt und programmiert werden,

(3) weisen oft eine geringe Skalierbarkeit auf

(4) und viele Kryptoprojekte sind überambitioniert.

(5) Folglich gibt es immer wieder digitale Cyberattacken.

Neben diesen technischen und wirtschaftlichen Hindernissen wird in diesem Kontext oftmals auch der hohe Energiebedarf der Kryptowährungen genannt. Dieses moralische Problem ist aus Natur- und Umweltschutzgedanken zu Recht zu betonen. Jedoch dürften unsere sonstigen alltäglichen Konsumgewohnheiten in puncto Energieverschwendung die Kryptowährungen wohl noch übertreffen.

Wie teuer sind Blockchain-Lösungen?

Blockchains sind extrem teuer. Jüngst hat der wohl bekannteste Kryptoentwickler nach Satoshi Nakamoto, der Gründer von Ethereum, Vitalik Buterin, die Kosten berechnet.[5] Seiner Berechnung nach ist die Ethereum-Blockchain rund eine millionmal teurer als zentralisierte Webserver. Ursächlich hierfür ist der hohe Synchronisationsbedarf aller Server in einer Blockchain. Eine Blockchain speichert neben der kryptografischen Verschlüsselung auch deshalb zuverlässig und unveränderbar eine Information, weil es hunderte oder tausende Kopien gibt. Entsprechend hoch ist der Synchronisationsbedarf und entsprechend aufwändig und kostspielig sind potenzielle Systemänderungen.

[5] Buterin, Vitalik (2018). Blockchains and Tradeoffs. Deconomy Day2. https://www.youtube.com/watch?v=JQ8SoCd0n3c

Entwickler und Programmierer sind rar und daher teuer

Doch der hohe Synchronisationsbedarf, ebenso wie die Anwendung von Kryptografie – und dies alles in einem komplett auf Konsens setzenden Ökosystem – erklärt die systeminhärente Komplexität von Blockchain-Lösungen. Entsprechend gibt es wenige Entwickler und Programmierer, die die Systeme pflegen und weiterentwickeln können. Die vielen hundert Kryptoprojekte konkurrieren folglich um wenige Spezialisten. Besonders begehrt sind dabei Solidity-Programmierer. Solidity ist eine der wichtigsten Computersprachen, um Smart Contracts zu programmieren. Die Sprache selbst ist erst zusammen mit der Kryptowährung Ethereum vor wenigen Jahren entstanden. Entsprechend sind viele Funktionalitäten, die in anderen Sprachen Standard sind, noch nicht implementiert oder die Dokumentation ist noch nicht vollständig. Das Programmieren mit Solidity ist also eine Herausforderung, weshalb die raren Solidity-Programmierer exzellent bezahlt werden.

Blockchains haben geringe Skalierbarkeit

Eine schnelle Massenadaption der Blockchain-Technologie ist schon deshalb nicht zu erwarten, weil die Transaktionskapazität bisher gering ist. Während die zentralisierten Bezahlsysteme täglich mehrere tausend Transaktionen pro Sekunde und in Stoßzeiten auch mehrere 10.000 Transaktionen pro Sekunde abwickeln können, stoßen die dezentralisierten Kryptowährungen aktuell bei einbestenfalls zweistelligen Transaktionen pro Sekunde an ihr Limit. Um diese technologische Grenze zu erhöhen, wird eifrig an Lösungen gefeilt. Es gibt zahlreiche Ansätze, um mehr Transaktionen pro Sekunde zu ermöglichen. Das bekannteste dürfte das eingangs bereits diskutierte Lightning Network sein. Dabei könnte die Skalierbarkeit insbesondere über die Vernetzung von Lightning Technologien verschiedener Kryptowährungen rasant ansteigen. Angesichts der weit über den Zahlungsmittelsektor hinausgehenden Anwendungsmöglichkeiten von Blockchains – wir erinnern an unsere Diskussionen rund um Internet of Things, Smart Contracts, künstliche Intelligenz etc. – wären auch die heutigen zentralisierten Zahlungsverkehrssysteme nicht leistungsfähig genug. Denn man benötigt womöglich mehrere Millionen Transaktionen pro Sekunde, um viele der oben beschriebenen Technikträume zu realisieren. Die schnelle und weitreichende Umsetzung von Blockchain-Projekten dürfte also noch einige Zeit allein an der fehlenden technologischen Skalierbarkeit scheitern.

Viele Kryptoprojekte sind überambitioniert

Es gibt bereits eine ganze Reihe von Kryptoprojekten, die nie das Licht der Welt erblickten. Andere Projekte, oft initiiert von sehr ambitionierten, relativ jungen Unternehmern, starten mit viel Elan, ohne anschließend wesentliche Fortschritte zu machen. Selbst relativ bekannte Projekte verfehlen immer wieder ihre selbst gesteckten Ziele. Einen hohen Bekanntheitsgrad weisen nur ganz wenige Kryptowährungen auf, eine hohe Marktdurchdringung kann wohl keine Blockchain-Lösung vorweisen und von relativ vielen Projekten ist nur noch ein Eintrag bei deadcoins.com übrig. Neben der Komplexität der Blockchain-Technologie sind für diese Fehlentwicklung, vor allem überambitionierte Ziele und fehlende Projektmanagement-, aber auch Lebenserfahrung anzuführen. So wollen einige Projektentwickler nicht nur die Blockchain-Technologie von Bitcoin verbessern, sondern gleichzeitig von der binären – also der Strom fließt oder fließt nicht – Hardware-Architektur auf eine tertiäre Architektur umstellen. Andere Projektentwickler träumen direkt von der Erschaffung eines Weltcomputers. Wahrscheinlich ist das die eine oder andere Revolution zu viel. Diese Projekte nutzten einfach den Hype der letzten Jahre aus, um schnell Geld einzusammeln. Mit dem

Preisrückgang der letzten Monate sind bereits einige Träume geplatzt. Um die guten von den schlechten Projekten zu unterscheiden, bedarf es trotzdem einer hohen Fachkompetenz und dies nicht nur in Krypto- und IT-Fragen, sondern auch in puncto Marktdurchdringung beim Endkunden. Angesichts der vielen schlecht gesteuerten Projekte stellt sich unserer Ansicht nach die Frage, ob diese Entwicklungen letztlich nicht auch zu einem Systemversagen führen könnten. Denn viele Kryptosysteme sind technisch miteinander verbunden. Fehler in den Schnittstellen einzelner Kryptoprojekte und Kryptowährungen könnten letztlich nicht nur einen psychologischen, sondern auch einen technischen Preiseffekt haben.

Folglich gibt es immer wieder digitale Diebstähle

Ein libertäres Prinzip ist die individuelle Eigenverantwortung. Die Verwendung außerstaatlichen Geldes impliziert damit direkt die persönliche Verwahrung und Verwaltung von PIN und TANs, also der Passwörter der digitalen Geldbeutel, den sogenannten Wallets. Da der Verlust von Zugangscodes ein alltägliches Phänomen ist, dürften sich auf absehbare Zeit nur wenige Menschen für die eigenverantwortliche Verwahrung von Kryptowährungen begeistern. Aufgrund der überambitionierten Projekte, aber ebenso aufgrund der fehlenden Zahl von Blockchain-Experten und dem damit einhergehenden fehlerhaften Programmiercode ist die Zahl der gestohlenen Kryptowährungen kräftig angestiegen. Mit diesen Diebstählen wird der libertäre Traum zum Alptraum.

Weitere Gründe für eine nur schleichende Blockchain-Revolution

Neben diesen systemimmanenten Hindernissen für eine schnelle Adaption gibt es eine Reihe weiterer Nachteile, die eine baldige Blockchain-Revolution unwahrscheinlich machen.

(1) Eine zu schnelle Adaption von dezentralen Lösungen hätte ein hohes disruptives Potenzial für die heutige Arbeitswelt und Gesellschaft.

(2) Blockchains sind für den potenziellen Nutzer unsichtbar und diese daher schwer zu überzeugen.

(3) Auch das Internet erfüllte viele revolutionäre Erwartungen nur teilweise.

Das hohe disruptive Potenzial der Dezentralität kann abschrecken

Durch das Speichern von Informationen auf Blockchains können viele Kontrollfunktionen und administrative Tätigkeiten, zum Beispiel Behördengänge, in der Zukunft überflüssig werden. Zum Beispiel wenn die Blockchain-Technologie zum Speichern digitaler Identitäten genutzt wird. Entsprechend könnten viele traditionelle Arbeitsfelder und Jobs überflüssig werden. Wenngleich durch Digitalisierung und die Einführung von Blockchains auch viele neue Jobs entstehen dürften, könnten bei einer zu schnellen Adaption weite Teile der Bevölkerung gegen die neuen Technologien votieren. Ein ähnlich disruptives Potenzial auf die Arbeitswelt und Gesellschaft dürfte auch von einer sehr schnellen Adaption von Kryptowährungen als globales Zahlungsmittel ausgehen. Wenn das heutige Nischenzahlungsmittel Bitcoin plötzlich bei neuen Verträgen eine hohe Relevanz aufwiese und sich global etablieren würde, dann könnte dies ungeahnte Folgen mit sich bringen. Müssten bei einer globalen Massenadaption alte Arbeits- und Rentenverträge auf Bitcoin umgestellt werden? Wenn ja, zu welchem Kurs? Wie würde die Besteuerung einer globalen, dezentralen Währung erfolgen? Derart grundlegende Fragen dürften bei vielen Menschen eher Angst als Begeisterung auslösen. Die von manchen herbeigesehnte globale Revolution

dürfte bei einer rasanten Massenadaption von vielen Menschen genauso rasant und strikt abgelehnt werden.

Blockchains sind hauptsächlich ein abstraktes Konstrukt

Oftmals wird die gesellschaftliche Wirkung der Blockchain-Technologie mit dem Internet verglichen. Da man Informationen auf einer Blockchain unveränderbar speichern kann, wirkt diese Technologie wie eine vertrauensbildende Maßnahme, selbst zwischen Fremden. Hier wird aber bereits der große Unterschied zwischen Blockchain und dem Internet deutlich. Denn Vertrauen ist ein abstrakter Begriff. Man kann Vertrauen weder sehen noch anfassen. Lediglich die mittelbaren Folgen von Vertrauen sind in Form von Handlungen beobachtbar. Das ist der große und womöglich entscheidende Nachteil bei einer Massenadaption der Blockchain-Technologie gegenüber dem Internet. Die Konsequenzen des Internets lassen sich dank der Übertragung von Bildern und Tönen unmittelbar erleben. Entsprechend war es leicht, auch Konservativen und Skeptikern die Vorteile zu verdeutlichen. Wenn sie als Nutzer eine Webseite besuchen, zum Beispiel um eine Flugverspätungsversicherung abzuschließen, bemerken sie keinen Unterschied zwischen einer Blockchain- und einer lediglich digitalen Lösung. Bei der Erzielung einer hohen Marktdurchdringung ist dies ein enormer Nachteil, denn während viele Experten von dem grundsätzlichen Potenzial der Blockchain-Technologie begeistert sind, weiß bis heute der Großteil der Bevölkerung nichts damit anzufangen.

Ambivalente Wirkung des Internets auf Freiheit und Demokratie

Anfang der 1990er Jahre wurde mit der Einführung des Internets viel über die Demokratisierung von Informationen gesprochen. Damals herrschte die Utopie vor, dass der universelle grenzüberschreitende Informationszugang und die damit verbundene Kommunikationsfreiheit eine gesellschaftliche Revolution auslöse. Zudem hoffte man auf eine intensivere Teilhabe am demokratischen Prozess. Denn jeder könne Leser, Editor, Autor von politischen Beiträgen, Initiator von Abstimmungen und Wähler sein. Die naive Erwartung einer quasi automatischen Intensivierung von Freiheit und Demokratie erfüllte sich nicht. Vielmehr hat das Internet, womöglich mehr als jede andere Technologie, zu einer stärkeren Differenzierung der Gesellschaft beigetragen. Die Marktmacht der großen Internetfirmen und ihrer geschlossenen Plattformen, den sogenannten „Walled Gardens“, werden zunehmend negativ wahrgenommen. Entsprechend werden die Auswirkungen auf Freiheit und Demokratie heute durchaus ambivalent bewertet.

Zusammenfassung und Ausblick

Es gibt immer noch sehr wenige Menschen, die das Potenzial von Bitcoin und Blockchain erfasst haben. Doch alle, die dieses Potenzial wenigstens erahnen und beginnen, die potenziellen gesellschaftlichen Auswirkungen der neuen Technologie zu erfassen, sind im positiven Sinne infiziert. Begeistert von der Vorstellung, in einer Welt zu leben, in der eine Technologie Vertrauen schafft bzw. einen Vertrauensmissbrauch verhindert. Wenngleich wir die Euphorie teilweise teilen, haben wir auch zahlreiche Restriktionen aufgezeigt. Diese dürften zumindest auf kurze Sicht, womöglich aber auch über Jahre hinweg die Blockchain-Revolution bremsen[6]. In der Zwischenzeit arbeiten nicht nur die Macher der Kryptowährungen, sondern auch viele Unternehmen und staatliche Institutionen daran, die neue Technologie in ihre bestehenden Geschäftsfelder und den regulatorischen Rahmen einzubetten. Wie bei der Internetrevolution könnte schließlich ein Großteil der Angebote von privater Seite kommen. Die Blockchain-Welt von morgen könnte, analog zu der Internet-Revolution in den letzten Jahrzehnten, deutlich ambivalentere gesellschaftliche Auswirkungen haben, als es die Enthusiasten heute erwarten.

Jochen Möbert (+49 69 910-31727, jochen.moebert@db.com)

[6] Ahrens, Tobias (2018): Wer gewinnt das Rennen um die Blockchain-Revolution?, Capital.de

Deutsche Bank
Research

EU-Monitor

„ Die multiplen Stufen der Blockchain-Revolution – oder einmal Kryptohype und zurück ..... 22. November 2018

„ Digitale Infrastruktur: Engpässe hemmen Europa ..... 28. September 2018

„ PSD 2, Open Banking und der Wert personenbezogener Daten ..... 19. Juni 2018

„ Digitale Wirtschaft: Wie künstliche Intelligenz und Robotik unsere Arbeit und unser Leben verändern ..... 18. Mai 2018

„ Reform des Gemeinsamen Europäischen Asylsystems: Ein schwieriges Unterfangen ..... 12. April 2018

„ Warum sollten wir Krypto-Euros nutzen? Digitales Bargeld von der Notenbank – die Sicht der Nutzer ..... 8. März 2018

„ EU-Haushalt nach dem Brexit: Streit ist vorprogrammiert ..... 2. März 2018

Unsere Publikationen finden Sie unentgeltlich auf unserer Internetseite www.dbresearch.de
Dort können Sie sich auch als regelmäßiger Empfänger unserer Publikationen per E-Mail eintragen.

Für die Print-Version wenden Sie sich bitte an:
Deutsche Bank Research
Marketing
60262 Frankfurt am Main
Fax: +49 69 910-31877
E-Mail: marketing.dbr@db.com

Schneller via E-Mail:
marketing.dbr@db.com

© Copyright 2018. Deutsche Bank AG, Deutsche Bank Research, 60262 Frankfurt am Main, Deutschland. Alle Rechte vorbehalten. Bei Zitaten wird um Quellenangabe „Deutsche Bank Research“ gebeten.
Die vorstehenden Angaben stellen keine Anlage-, Rechts- oder Steuerberatung dar. Alle Meinungsaussagen geben die aktuelle Einschätzung des Verfassers wieder, die nicht notwendigerweise der Meinung der Deutsche Bank AG oder ihrer assoziierten Unternehmen entspricht. Alle Meinungen können ohne vorherige Ankündigung geändert werden. Die Meinungen können von Einschätzungen abweichen, die in anderen von der Deutsche Bank veröffentlichten Dokumenten, einschließlich Research-Veröffentlichungen, vertreten werden. Die vorstehenden Angaben werden nur zu Informationszwecken und ohne vertragliche oder sonstige Verpflichtung zur Verfügung gestellt. Für die Richtigkeit, Vollständigkeit oder Angemessenheit der vorstehenden Angaben oder Einschätzungen wird keine Gewähr übernommen.
In Deutschland wird dieser Bericht von Deutsche Bank AG Frankfurt genehmigt und/oder verbreitet, die über eine Erlaubnis zur Erbringung von Bankgeschäften und Finanzdienstleistungen verfügt und unter der Aufsicht der Europäischen Zentralbank (EZB) und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) steht. Im Vereinigten Königreich wird dieser Bericht durch Deutsche Bank AG, Filiale London, Mitglied der London Stock Exchange, genehmigt und/oder verbreitet, die von der UK Prudential Regulation Authority (PRA) zugelassen wurde und der eingeschränkten Aufsicht der Financial Conduct Authority (FCA) (unter der Nummer 150018) sowie der PRA unterliegt. In Hongkong wird dieser Bericht durch Deutsche Bank AG, Hong Kong Branch, in Korea durch Deutsche Securities Korea Co. und in Singapur durch Deutsche Bank AG, Singapore Branch, verbreitet. In Japan wird dieser Bericht durch Deutsche Securities Inc. genehmigt und/oder verbreitet. In Australien sollten Privatkunden eine Kopie der betreffenden Produktinformation (Product Disclosure Statement oder PDS) zu jeglichem in diesem Bericht erwähnten Finanzinstrument beziehen und dieses PDS berücksichtigen, bevor sie eine Anlageentscheidung treffen.

Druck: HST Offsetdruck Schadt & Tetzlaff GbR, Dieburg

ISSN (Print): 1612-0256; ISSN (Online): 1612-0264