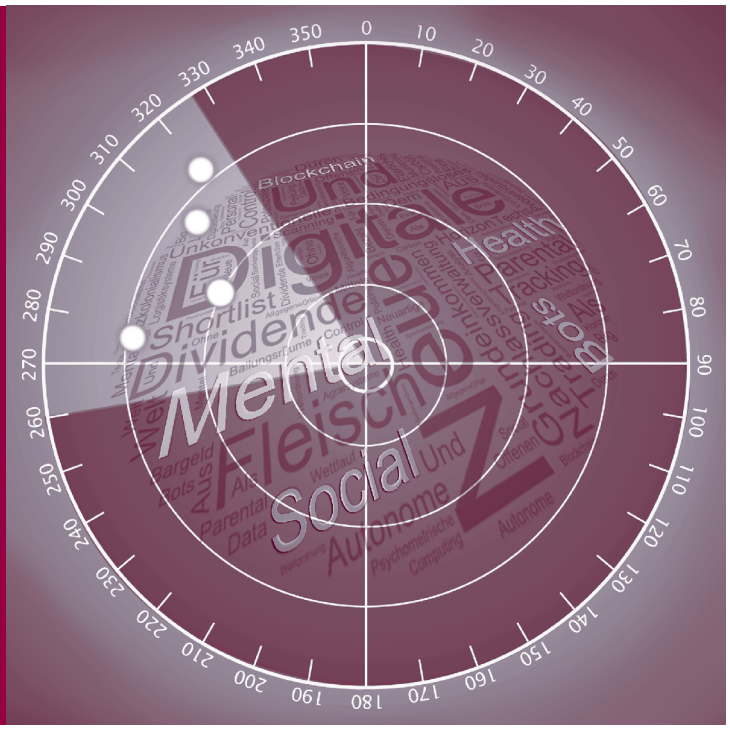
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Daniel Thiele
Simone Ehrenberg-Silies

Blockchain



Themenkurzprofil Nr. 1
Mai 2016

Blockchain

Kurzdarstellung des Themas

Die Blockchain (Blockkette) ist die technologische Grundlage von neuartigen digitalen Zahlungssystemen (auch Kryptowährungen genannt), wie z. B. Bitcoins. Der Grundgedanke der Blockchaintechnologie ist es, eine nachvollziehbare, dezentral organisierte, unverletzliche und damit fälschungssichere Möglichkeit zu schaffen, um Transaktionen abbilden zu können, ohne auf eine zentrale Organisation oder Mittelsmänner wie Banken, Notare oder Treuhänder zurückgreifen zu müssen (Casey/Vigna 2015, Kap. 1, S. 1). Das Vertrauen in die korrekte Abwicklung der Transaktionen wird auf technologischem Wege mittels digitaler Signaturen und Verschlüsselungstechnologien erzeugt.

Blockchain ist eine Basistechnologie, die weit über den ursprünglichen Anwendungsfall Kryptowährungen hinaus in allen Bereichen, in denen es um die Feststellung bzw. Übertragung von Eigentum an digitalen bzw. digitalisierbaren Gütern geht, eingesetzt werden könnte. Hierzu zählen u. a. Wertpapierhandel, öffentliche Register (z. B. Grundbücher), elektronische Wahlen aber auch neuartige Konstrukte wie sich selbst vollziehende Verträge (Smart Contracts). Von Fachleuten wird der Technologie ein erhebliches disruptives Potenzial zugesprochen.

In einer Blockchain sind sämtliche jemals getätigten Transaktionen aller Nutzer, am Beispiel der Bitcoins – Kauf und Verkauf – in dezentraler Form in einem Peer-to-Peer-Netzwerk gespeichert. Neue Transaktionen werden an die bestehende Kette von Datenblöcken als neuer Datenblock angehängt. Die übertragenen Daten werden mithilfe eines speziellen Verfahrens kodiert, sodass ein unbefugter Eingriff in die Daten nicht möglich ist. Die Blockchain im Falle der Bitcoins ist somit vergleichbar mit einer öffentlich einsehbaren Buchhaltung eines Unternehmens, die alle Geschäftsvorgänge beinhaltet (Swan 2015, S. X). Jeder Block entspricht in dieser Analogie einer Seite in dem Transaktionsjournal.

Hintergrund und Stand der Entwicklung

Das Konzept der Blockchain wurde 2008 im Zusammenhang mit der Entwicklung der Bitcoinwährung als digitales Zahlungsmittel entwickelt (Nakamoto 2008, S. 1 f.). Die Blockchain lässt sich als digitales Register beschreiben, in dem alle Transaktionen seit Beginn der Nutzung der Technologie festgeschrieben werden. Oberstes Ziel der Entwicklung der Blockchaintechnologie war es, finanzielle Interaktionen ohne den Einsatz von Dritten zwischen zwei Akteuren,

die sich weder kennen, noch vertrauen müssen, durch den Einsatz von Technologie billiger, schneller und sicherer durchführen zu können, und dies unabhängig von staatlich oder anderweitig regulierten Instanzen (Gundlach 2015; www.gruenderszene.de/lexikon/begriffe/blockchain [25.4.2016]; http://lexicon.ft.com/PrintTerm?term=blockchain [25.4.2016]). Das Verfahren fußt auf einem ausgeklügelten Algorithmus zur Verifizierung von Transaktionen So hat das zugrundeliegende Netzwerk eine dezentrale Peer-to-Peer-Struktur und nutzt keine zentralen Server. Informationen werden im Netzwerk unter allen Akteuren öffentlich geteilt und allen Akteuren gleichzeitig zugänglich gemacht. Weiterhin werden alle Transaktionen in Form von Datenblöcken[1] gespeichert. Diese Datenblöcke werden mit einem Kodierungsverfahren bearbeitet und unter allen Teilnehmern verifiziert.

Ähnlich dem Public-Key-Verschlüsselungsverfahren erzeugt jeder Teilnehmer ein zusammenhängendes Schlüsselpaar, einen privaten (geheim zu haltenden) und einen öffentlichen (breit publizierten). Eine Transaktion wird mit dem privaten Schlüssel signiert und ist mit dem öffentlichen Schlüssel lesbar. Jede Transaktion kann eindeutig einem öffentlichen Schlüssel zugeordnet werden. Dieser dient somit als Pseudonym des Nutzers. Im Falle der Bitcoins entspricht dieser Schlüssel quasi der Kontonummer. Um die Transaktionen in eine eindeutige zeitliche Reihenfolge zu bringen, werden diese in Blöcken angeordnet, die mit einem kryptografischen Verfahren so aneinander geknüpft werden, dass eine nachträgliche Veränderung nicht mehr möglich ist.[2] Jeder neue Datenblock baut auf der aktuellen Transaktion als auch auf dem Block der zuletzt getätigten Transaktionen auf. Dadurch entsteht eine Kette an kodierten Blöcken (die Blockchain), die sich bis zur allerersten Transaktion, aufbauend auf dem einzig fest kodierten Startblock (genannt Genesis Block), nachvollziehen lässt. Die Verifizierung einer Transaktion geschieht mit Durchführung der nächsten Transaktion, die aufbauend auf der Blockchain alle vorigen Transaktionen mit einbezieht, sodass eine Fälschung nahezu unmöglich ist. Alle Transaktionen können zudem öffentlich nachvollzogen werden[3], jedoch bleiben aufgrund der

1 Zum Tätigen von Transaktionen werden ständig neue, gültige und verifizierbare Datenblöcke erzeugt. Der Vorgang des Erzeugens eines neuen Datenblocks heißt Mining (Schürfen). Das mining erfordert eine hohe Rechenleistung, da entsprechend der Vorgaben des Algorithmus eine hohe Komplexität zur Gewährung der Sicherheit eingehalten werden muss. Die Bitcoin-Blockchain entlohnt deshalb Akteure (anteilmäßig) mit Bitcoins dafür, wenn sie Rechenleistung ihrer Computer dem Netzwerk zur Generierung neuer Datenblöcke zur Verfügung stellen (BTC-Echo).

2 Im Beispiel der Bitcoins wird die Hashfunktion SHA-256 genutzt (https://en.bitcoin.it/wiki/SHA-256; Studer 2010, S. 68 f.).

3 Ein Beispiel zur öffentlichen Einsichtnahme ist die Plattform https://blockexplorer.com/. Diese zeigt eine ständig aktualisierte Liste der zur Verfügung stehenden Datenblöcke für Transaktionen sowie die zuletzt getätigten Transaktionen und deren Höhe in Bitcoins an.

angewandten Verschlüsselungsmethode der jeweilige Absender und der Empfänger der Transaktion praktisch anonym.[4]

Die erreichte Verfügbarkeit, Stabilität und Sicherheit der Blockchaintechnologie bei der Abwicklung von Transaktionen ist mittlerweile vergleichbar mit dem heutigen Standard von Onlinekonten und zieht deshalb in jüngster Zeit nicht nur Akteure aus der Bankenbranche (Dapp et al. 2015) an, sondern bietet auch für Anbieter von Dienstleistungen in ähnlich transaktionsabhängigen Branchen neue Möglichkeiten.

In aktuellen Diskussionen und Fachbeiträgen der Finanzbranche findet die Blockchaintechnologie vor allem aufgrund ihres disruptiven Potenzials in Bezug auf das vorherrschende Banken- und Finanzsystem große Beachtung. Vor allem für die Abwicklung des internationalen Zahlungsverkehrs und für den Handel mit Wertpapieren wird die Blockchain als mögliche Zukunftstechnologie gesehen (Bundesverband deutscher Banken e. V. 2015, S. 11). So haben große, international agierende Finanzinstitute bereits erste Tests mit der Blockchaintechnologie in verschiedenen Bereichen des Finanzwesens durchgeführt (finews.ch 2015). Auch die US-amerikanische Zentralbank prüft unter dem Begriff Fedcoin derzeit, ob eine blockchainbasierte Komponente in ihre Geldpolitik integriert werden könnte (Koning 2014).

Weitere Anwendungsbereiche der Blockchaintechnologie sind überall dort denkbar und sinnvoll, wenn die zu verwaltenden Transaktionen hohe Anforderungen an Transparenz, Integrität und Nachvollziehbarkeit aufweisen und gleichzeitig geringe Kosten bei der Bewältigung von großen Datenaufkommen realisiert werden müssen (Grollmann 2016; Swan 2015).

Mit der Weiterentwicklung der Blockchaintechnologie, die ursprünglich zur Realisierung der Bitcoins und damit zur Schaffung der ersten digitalen und dezentralisierten Währung erschaffen wurde, hin zur Blockchain 2.0 (Swanson 2014) wurde der Grundstein dafür gelegt, ganze Märkte zu dezentralisieren (Swan 2015, S. 9). Die Blockchain 2.0 erlaubt es, verschiedenste Angebote und Dienstleistungen zu entwickeln, die auf den zentralen Eigenschaften der Blockchaintechnologie aufbauen und diese um neue Eigenschaften[5] ergänzen.

---

4 Dennoch ist es nicht unmöglich, einen Nutzer z. B. über die verwendete IP-Adresse oder über die Analyse von Nutzungsmustern zu identifizieren. Eine stärkere Anonymität kann darüber hinaus durch Verschleierungsverfahren generiert werden (z. B. eine Anonymisierung über das Tor-Netzwerk).

5 Merkmale, die mit der neueren Blockchaintechnologien ermöglicht werden, sind u. a. das sogenannte Multi-Signature-Feature, welches Transaktionen nur dann als gültig bestätigt, wenn mindestens zwei Personen (bzw. der überwiegende Anteil einer größeren, vordefinierten Gruppe [M-of-N-Transaktionen]) diese bestätigen. Ebenso können Transaktionen mit der Lock-Time-Funktion für eine bestimmte Zeit gesperrt bzw. zu einem vorbestimmten Zeitpunkt ausgelöst werden (Rotzoll 2016).

Erste Anbieter wie die Stiftung Ethereum (www.ethereum.org), Codius (https://codius.org/) oder Nxt (https://nxtplatform.org/) ermöglichen die Nutzung der (z. T. anbietereigenen) Blockchain-2.0-Technologie und eröffnen eine globale Plattform für neue Angebote mit disruptivem Charakter: Täglich entstehen auf diese Weise neue Dienstleistungen zur Abwicklung von Smart Contracts[6], für den Handel mit Wertpapieren, Vermögensgegenständen und Kapitalanlagen sowie für Angebote, die Identitätsnachweise (z. B. Personalausweis, Führerschein) bedürfen. Ebenfalls werden einerseits unabhängige (https://bitnation.co/) und anderseits auch staatliche E-Governmentlösungen (Cabinet Office et al. 2016) entwickelt, beispielsweise für die Beglaubigung von Urkunden, die Teilnahme an Abstimmverfahren und Wahlen, der Hinterlegung von Testamenten, Versicherungsabschlüsse etc. (EtherCasts 2016; Grollmann 2016; Swan 2015, S. 10 ff.).

Auch die Verbindung zwischen der digitalen Welt und der physischen Welt kann mit der Blockchain-2.0-Technologie geschaffen werden: so bietet die Firma Slock.it eine Lösung an, die, aufbauend auf der Authentifizierung via Blockchain, Schlösser öffnet (Slock.it UG 2016).

Die Blockchaintechnologie ist aufgrund der technischen Rahmenbedingungen jedoch nicht per se für alle Anwendungszwecke geeignet. Da alle Transaktionen in Blöcken gespeichert werden, die erst von den am Miningprozess beteiligten Akteuren der jeweiligen Blockchain generiert werden müssen, ist die Performance einer Blockchaintransaktion im Vergleich zu den heute möglichen Performancewerten von anderweitig organisierten Datenbanksystemen sehr gering[7]. Durch eine Veränderung der Blockgröße könnten Performancegewinne erzielt werden, die gleichzeitig mit einer Zentralisierung einhergehen würden, was dem ursprünglichen Zweck der Einführung der Blockchaintechnologie widerspricht (Rotzoll 2016).

---

6 Der Begriff Smart Contracts (intelligente Verträge) wurde 1994 von Nick Szabo begründet und meint die vollständig automatisierte Abwicklung von digital erfassten Verträgen. Tritt eine vorerfasste Vertragskonstallation (Trigger) ein, werden automatisch die für diesen Fall vorbestimmten und im Programmcode festgelegten Handlungen vom Computersystem durchgeführt. Smart Contracts sind aufgrund ihrer digitalen Handlungsweise frei von emotionalen Entscheidungen und bergen das große Potenzial, vorbestimmte, rationale, faire und transparente Entscheidungen ohne den Einsatz von Dritten vollkommen automatisiert nach vordefinierten Regeln abzuwickeln. Auf diese Weise können neuartige Geschäftsbeziehungen realisiert und typischerweise auftretende Transaktionskosten gesenkt werden (Szabo 1994; Cassano 2014; He et al. 2016, S. 23).

7 In der Bitcoin-Blockchain lassen sich im Durchschnitt nur sieben Transaktionen pro Sekunde durchführen während relationale Datenbanken auch bei großen Datenmengen mehr als 30 Transaktionen pro Sekunde durchführen können (Rotzoll 2016).

Im Laufe der Zeit haben sich neben der für die Währung Bitcoin entwickelten Blockchain viele weitere Blockchains[8] und Kryptowährungen entwickelt, deren gesamte Marktkapitalisierung mehr als 8,6 Mrd. US-Dollar umfasst (CoinMarketCap 2016). Während die Bitcoin-Blockchain eher kleinen, konservativen Veränderungen über den Zeitverlauf unterlegen war, existieren andere Blockchains der sogenannten Blockchain-2.0-Technologie, wie beispielsweise die Ethereum-Blockchain (www.ethereum.org), die im Vergleich dazu größere Freiheit (bei höherer Komplexität) für Entwickler und Anbieter von neuen Dienstleistungen bietet.

Die Vielfältigkeit an Blockchains und die Vielfältigkeit der Anwendungsmöglichkeiten wird in Zukunft weiter zunehmen. Es ist deshalb auch davon auszugehen, dass durch die stetige Vergrößerung der Nutzerzahl, die Vergrößerung des investierten Kapitals, die hohen technologischen Sicherheitsstandards und durch die gleichzeitig niedrigen Einstiegsbarrieren die Akzeptanz der Blockchaintechnologie bei regulierten Institutionen und insbesondere auch bei staatlichen Institutionen und Organen zunehmen wird.

Erst die Einbettung der Blockchaintechnologie in einen gesicherten rechtlichen Rahmen, wie es beispielsweise für Großbritannien in der E-Governmentlösung GOV.UK geprüft wird (Cabinet Office et al. 2016), wird zu den bereits vieldiskutierten, disruptiven Veränderungen führen können, da eine Technologie, die keine Anknüpfungspunkte an das geltende öffentliche Recht hat, anderenfalls nur ein Nischendasein führen wird (Rotzoll 2016). Wird die Technologie in naher Zukunft in verschiedenen Anwendungen im öffentlichen Sektor eingesetzt, geschieht dies erst dann, wenn die Klärung der rechtlichen Rahmenbedingungen zum Einsatz der Technologie abgeschlossen ist. Mit dem erfolgreichen Einsatz in der öffentlichen Verwaltung und in E-Governmentlösungen wird die Anwendung der Blockchaintechnologie auch in die Breite der Bevölkerung transportiert, was der Technologie zu einer höheren Bekanntheit und zu breiterer Akzeptanz verhelfen kann.

Die zukünftige Entwicklung der Blockchaintechnologie hängt einerseits davon ab, in welchem Umfang es den Entwicklern der verschiedenen Blockchaintechnologien gelingt, die Technologie weiterhin zu verbessern und an die wechselnden Bedürfnisse der Anwender anzupassen, ohne dabei die inhärenten und für die Nutzer so essenziellen Merkmale des Gesamtsystems zu gefährden. Andererseits hängt die Zukunft der Blockchaintechnologie auch davon ab, in welchem Maße Akteure aus den konservativen, transaktionsabhängigen und regulierten Branchen, beispielsweise aus dem Bankensektor oder dem Börsenhandel,

8 Die Website CoinMarket Cap (2016) listet 690 Kryptowährungen und 57 Dienste (Assets), die alle mit eigenen Blockchains operieren (Stand: 27.4.2016).

die Potenziale der Technologie erkennen, diese für ihre Zwecke entdecken und ggf. für eigene Anwendungen und neue Dienstleistungen nutzen.

Auch die zukünftige Entwicklung der Akzeptanz und Verbreitung von Kryptowährungen, deren Basis die Blockchaintechnologie ist, hat maßgeblichen Einfluss auf die Technologie. Durch die im Kodierungsalgorithmus genutzte mathematische Beschränkung, mit deren Hilfe sowohl die Sicherheit, Anonymität und Verifikation des Systems sichergestellt wird und mit der neue Datenblöcke und Bitcoins durch das mining erzeugt werden, stellt eine fest implementierte Obergrenze[9] der verfügbaren Währungseinheiten dar. Diese Obergrenze wirkt vertrauensbildend und eher deflationär als inflationär, da – anders als bei konventionellem Geld – neue Einheiten (z. B. Banknoten) nicht einfach nachgedruckt werden können.[10] Die zukünftige Akzeptanz der Blockchaintechnologie wird auch davon gekennzeichnet sein, inwieweit sie sich von Anwendungen im kriminellen Milieu emanzipieren kann und inwieweit sich Skandale um virtuelle Währungen und Marktplätze verhindern lassen. Erste Erfolge gegen die organisierte Kriminalität konnte das FBI 2013 und 2014 mit der Schließung der bekanntesten digitalen Marktplätze für Drogen, Waffen und krimineller Dienstleistungen im Internet, der sogenannten Silk Road (Seidenstraße) und deren Nachfolger Silk Road 2, erzielen (Cox 2014; Die Zeit 2013). Mit der Verhaftung und Überführung des CEO von Mt. Gox[11] durch die Polizei in Tokyo wurde der bis heute größte Missbrauchsskandal einer Kryptowährung aufgeklärt, bei dem zwischenzeitlich[12] ein Schaden von umgerechnet ca. 450 Mio. US-Dollar entstand (D'Orazio 2015). Aktuelle Skandale, wie z. B. der durch einen Hacker verursachte Diebstahl von mehr als 50 Mio. US-Dollar in der Blockchain Ethereum

9 Die theoretisch maximal verfügbare Anzahl an Bitcoins liegt bei ca. 21 Mio. Bitcoins. Nach und nach werden diese über den Prozess des Minings erzeugt. Durch stetige Anpassung der Schwierigkeit des Miningalgorithmus wird die maximale Zahl jedoch erst im Jahr 2140 erreicht sein (Platzer 2014, S. 155).

10 Durch die relativ große Verbreitung der Kryptowährungen und die damit auch gestiegene Anzahl von Minern wurde die anfänglich vorhandene Gefahr einer Monopolbildung durch übermäßig erfolgreiche Schürfer reduziert, die durch die Bereitstellung von Rechenleistung mit Bitcoins entlohnt werden, da der Wert der Bitcoins, die für das erfolgreiche Durchlaufen des Miningprozesses verteilt werden, mittlerweile geringer ist, als die Stromkosten, die während des minings auftreten, und sich so kein direkter kommerzieller Nutzen aus der Beteiligung am mining ergibt (Conrad 2013). Tatsächlich kann es über die Zeit sogar zu Verlusten und zur Absenkung der Menge an Bitcoins kommen, beispielsweise durch Zerstörung von Festplatten oder Verlust von physischen Bitcointrägern (Wallets). Da die Anzahl der Währungseinheiten begrenzt ist, und durch Verlust sogar leicht rückläufig, können Bitcoins eine eher deflationäre Entwicklung nehmen – und im Wert steigen (Weiss 2014).

11 einem der ehemals wichtigsten Onlinehandelsplätze für Bitcoins

12 Mt. Gox gab 2014 an, dass von den 850.000 verschwundenen Bitcoins, eine Summe von 200.000 Bitcoins, zum damaligen Zeitpunkt umgerechnet ca. 100 Mio. US-Dollar, wieder aufgetaucht sei (Kastrenakes 2014).

beim Unternehmen DAO, zeigen, dass auch heute noch große Herausforderungen in der Absicherung von Blockchains gegenüber Angriffen von außen bestehen, die im Sinne der Schaffung von Vertrauen und der damit verbundenen breiten Akzeptanz der Technologie, gelöst werden müssen (Locker 2016).

Gesellschaftliche und politische Relevanz

Derzeit befindet sich die Blockchaintechnologie noch in einem vergleichsweise frühen Stadium: Der Kreis der Nutzer ist noch sehr eingeschränkt. Während nur in Ansätzen ein gesellschaftlicher Diskurs über die Potenziale der Blockchaintechnologie stattfindet, findet ein Großteil der Debatten über die Technologie im Kreis der hauptsächlichen Akteure, d. h. der Entwicklungs- und Anwendercommunity, über Internetplattformen und in Form von Thinktanks statt. Die einzig nennenswerte Diskussion in den Medien beschäftigt sich meist mit den Chancen und Risiken der Bitcoinwährung, sowie mit den z. T. illegalen Handelsplätzen (Schulz 2016a u. 2016b; Wetzel 2016). Neben den Auswirkungen, die die Nutzung der Bitcoins auf das Bezahlen im Alltag hat, werden häufig vor allem die Potenziale und Gefahren der Technologie diskutiert, die vor allem von Akteuren des Banken- und Versicherungssektors mit kritischem Blick verfolgt werden (Bundesverband deutscher Banken e. V. 2015, S. 10; Dapp 2016; Storm 2015).

Zwei Charakteristika der Blockchaintechnologie sind geeignet, massive gesellschaftlich relevante Implikationen auszulösen: Erstens, dass mit Nutzung der Technologie vormals vom Staat (bzw. von Intermediären wie Banken, Notare etc.) ausgefüllte Funktionen zu gewissen Teilen durch das gemeinschaftliche Vertrauen in ein offenes, gemeinsam akzeptiertes Protokoll ersetzt wird, welches sowohl den öffentlich einsehbaren Quellcode als auch die öffentlich einsehbaren Transaktionen einschließt. Zweitens führen die für die Blockchaintechnologie eingesetzten Verschlüsselungssysteme und die nachträgliche Unveränderbarkeit von Daten (Integrität) dazu, dass eine einmal durchgeführte Transaktion nicht wieder rückgängig gemacht werden kann (es gibt also keine Rückruffunktion, wie z. B. die Rückbuchung bei Lastschriftaufträgen). Außerdem hat jede Person, die über den (geheim zu haltenden privaten) Schlüssel verfügt, volle Verfügungsgewalt (besitzt also quasi eine nicht sperrbare PIN und TAN-Liste für beliebige Transaktionen), d. h., dem Schutz des Schlüssels kommt eine essentielle Bedeutung zu.

Die zukünftige Entwicklung der Blockchaintechnologie hängt von vielen Faktoren, Rahmenbedingungen und Akteursgruppen ab, deren Einfluss aus heutiger Sicht noch nicht vollständig absehbar ist.

Wird die Blockchaintechnologie wie bisher in den meisten Fällen in der Vergangenheit weiterhin dazu genutzt, um sichere, anonyme und dezentrale Netzwerke zu etablieren, kann die Technologie die Akzeptanz und Wahrnehmung von traditionellen Branchen und Strukturen, wie beispielsweise die der Banken und Versicherungen, verändern, da mithilfe von Kryptowährungen und Smart Contracts keine zentralisierten Geldinstitute oder Vertragsverwaltungsorganisationen mehr benötigt werden, um Vertragsinhalte zwischen Personen und Institutionen zu gestalten und zu verwalten und um Gelder weltweit zu transferieren.

Mit der ständigen Weiterentwicklung der Blockchaintechnologie, ermöglicht durch die freie Verfügbarkeit des Quellcodes, und mit der fortschreitenden Spezialisierung von Hardwareherstellern, die immer besser auf die Anforderungen der Miningprozesse zugeschnittene Hardware bereitstellen, wird sich in Zukunft auch die Performance[13] von neuen Blockchains erhöhen. Die Bitcoin-Blockchain wird in Zukunft jedoch kaum spürbare Performancegewinne erzielen können, da die Schwierigkeit der dem Miningprozess zugrundeliegenden Berechnung des Hashwertes alle 2016 Datenblöcke mit dem Ziel angepasst wird, dass die Lösung der Aufgabe im Durchschnitt 10 Minuten dauert. Mit steigenden Performancewerten anderer Blockchains wird die Technologie dennoch verstärkt in den Fokus der Finanz- und Börsenwelt rücken, da das Arbeiten mit hohen Transaktionsraten einer der letzten Vorteile der heute verwendeten Technologien des traditionellen Bankensektors ist. Erreicht eine Blockchain annähernd diese Performancewerte, könnte sie durch ihre technologischen Merkmale und durch ihre vergleichsweise kostengünstige Umsetzung die Geschäftsmodelle der Banken langfristig bedrohen, wenn es den etablierten Akteuren nicht gelingt die Technologie für ihre Zwecke zu nutzen.

Effekte, die mit dem Einsatz der Blockchaintechnologie einhergehen würden, lägen vor allem in der Liberalisierung, Dezentralisierung und der als positiv bewerteten Erhöhung der Transparenz der Finanzverwaltung, mit denen neue Formen der Bezahlung, beispielsweise Micropayments oder erfolgsabhängige Start-up-Finanzierung[14], möglich wären. Weitet man den Blick auf Länder, in denen kein etabliertes Bankensystem vorhanden ist oder in denen keine demokratische Regierungsform herrscht, könnte die Nutzung der Blockhaintechno-

13 Anzahl der pro Sekunde realisierbaren Transaktionen

14 Erste Konzepte für erfolgsabhängige Finanzierungsrunden von Start-up-Unternehmen basieren auf der Überprüfung der erreichten Planwerte des zuvor definierten Businessmodells und Geschäftsplans und der automatischen Freigabe von Investorengeldern. Potenzielle Investoren müssen vorab einen Maximalbetrag ihrer gewünschten Investmentsumme über mehrere Investmentrunden festlegen. Zum Schutz der Investoren wird der Betrag für eine neue Runde aber nur dann weiter ausgeschöpft, wenn das Start-up-Unternehmen die definierten Schwellwerte der Kennzahlen nachweisen kann.

logie, insbesondere zu Zahlungszwecken und zur Verwaltung von Finanzen, ein großer Vorteil für die Bevölkerung werden.

Wird die Weiterentwicklung der Technologie maßgeblich von Institutionen mitbestimmt, die ein Interesse an der Auswertung der in der Blockchain transparent und fälschungssicher abgespeicherten Daten haben, werden diese die Informationen dazu nutzen, um ihrerseits Smart Contracts zu gestalten, dass bestimmte Verhaltensweisen der Vertragsnehmer (z. T. passiv; Stichwort Nudging) forciert werden. Dies führt insgesamt dazu, dass Verträge entwickelt werden, die in den meisten Fällen zum Vorteil der Vertragsanbieter und zum Nachteil der Vertragsnehmer ausgestaltet sind, da jede einzelne Handlung in der Blockchain protokolliert. Auf diese Weise können alle Daten in der Blockchain für nachfolgende Verträge bzw. Vertragsverhandlungen ausgewertet werden, beispielsweise im Rahmen der Prüfung der Kreditwürdigkeit von Personen (Dapp 2016).

Eine massenhafte Adoption einer Parallelwährung (Bitcoin o. Ä.) ohne staatliche Aufsicht hätte nicht nur massive Auswirkungen auf Fragen des Verbraucherschutzes[15], sondern es sind auch Systemrisiken (für den Bankensektor etc.) denkbar. Darüber hinaus könnten volkswirtschaftliche Risiken dadurch provoziert werden, dass der Wechselkurs der Bitcoins frei fluktuiert und die Zentralbanken die umlaufende Geldmenge nicht mehr steuern können.

Darüber hinaus bietet die Technologie noch weitere Anwendungsfelder, die die bisherigen Strukturen in verschiedenen Branchen verändern können: So existieren beispielsweise Bestrebungen und erste Konzepte, um mithilfe der Blockchaintechnologie Wahlprozesse durchzuführen (Dapp 2016); (Grollmann 2016). Ebenfalls eignet sich die Blockchain dazu, geistiges Eigentum zu verwalten und bisher durch Notare geleistete Dienstleistungen zu ersetzen (Grollmann 2016; Rotzoll 2016). Weiterhin könnten E-Governmentangebote entwickelt werden, die auf Basis der eindeutigen Identifikation einer Transaktion (und damit eines Nutzers) digitale Angebote für bürgernahe Dienstleistungen der Verwaltung, wie z. B. das Ausstellen oder die Beglaubigung von Dokumenten, ermöglichen (Cabinet Office et al. 2016).

Über die legalen Anwendungsfälle der Blockchaintechnologie hinaus ergeben sich jedoch auch weiterhin illegale Potenziale durch die Nutzung von Kryptowährungen, wie beispielsweise Geldwäsche, Drogen- oder Waffenhandel (Schulz 2016b). So sind Kryptowährungen heute das zentrale Zahlungsmittel (Martin 2014, S. 27) im sogenannten Dark Net, ein anonymes Untergrundinternet, abseits der von Suchmaschinen erreichbaren Seiten, welches seinerseits ein

15 Beispielsweise verloren Anleger etw 650.000 Bitcoin an Einlagen (nach heutigem Kurs etwa 300 Mio. Euro), als der seinerzeit größte Bitcoinhandelsplatz Mt. Gox Insolvenz anmeldete.

Peer-to-Peer-Netzwerk darstellt, das nur mit besonderen Hilfsmitteln[16] betreten und genutzt werden kann (Bartlett 2015, S. 2 ff.)[17].

Mit zunehmender Verbreitung von blockchainbasierten Dienstleistungen und der steigenden Kapitalisierung von Kryptowährungen kann es in Zukunft dazu kommen, dass sowohl die Bedeutung der traditionell vom Staat übernommenen Funktionen als auch die Bedeutung des regulierten Bankensystems sinkt, wenn die beteiligten Akteure die Technologie nicht frühzeitig für ihre Zwecke adaptieren und nutzbar machen. Es könnte untersucht werden, welche blockchainbasierten E-Governmentlösungen sich im Sinne eines Bürokratieabbaus eignen könnten, z. B. um Amtsgänge, wie z. B. das Ausstellen eines amtlich beglaubigten Dokuments, effizienter zu gestalten (Dapp 2016)[18].

Ferner sollte durch geeignete Anonymisierungsverfahren sichergestellt werden, dass die Nutzung der Blockchaintechnologie und die damit einhergehende absolute Transparenz über alle getätigten Handlungen bzw. Transaktionen nicht dazu führt, dass diese riesige Menge an Daten und Informationen – ohne das Wissen der Nutzer – dazu verwendet wird, um detaillierte Analysen zu Profilbildungszwecken durchzuführen, die sich nachteilig auf die Gestaltung und das Aushandeln von Verträgen, beispielsweise Kredit-, Versicherungs- und Gesundheitstarife, auswirkt.

Weiterhin sollten Initiativen ins Leben gerufen werden, die die Gesellschaft über die technologischen Hintergründe, den Nutzen, die Risiken und die Auswirkungen der Blockchaintechnologie informieren, um ein breites Verständnis und eine dringend benötigte Technologiekompetenz schaffen zu können – insbesondere in Bezug auf die neuen Anforderungen im Umgang mit Verschlüsselungsmechanismen (Stichworte: Verlust des privaten Schlüssels).

16 Mit der Einführung des Tor-Clients (Abk. für The Onion Router) im Jahr 2002 wurde das Dark Net als Peer-to-Peer-Netzwerk ermöglicht Dingledine/Mathewson (2002).

17 So wurde die Plattform Silkroad, über die hauptsächlich illegale Drogen und andere Waren gegen Bitcoin umgesetzt worden sind, 2014 in einer konzertierten Aktion von FBI und Europol zerschlagen.

18 Zum Beispiel nutzt Honduras die Bitcoin-Blockchain zur Einführung eines digitalen Katasteramtes zur Verwaltung von Landrechten und Grundstücksansprüchen. In der Vergangenheit wurden die zentralisierten, staatlichen Einrichtungen häufig zum Ziel von Hackern, denen es gelang, geltende Landrechte zu verändern. Zumeist haben Bürokraten von dem Landrechtsbetrug profitiert, da ihnen nach den Hackerangriffen die Landrechte an Stränden zugesprochen worden.

Mögliche vertiefte Bearbeitung des Themas

Aufgrund der Aktualität und der erheblichen gesellschaftlichen und politischen Relevanz bietet sich das Thema für eine Bearbeitung als TA-Projekt an. Ziel wäre es, den Stand von Technik und Entwicklung umfassend darzustellen sowie einen Überblick über die wichtigsten Blockchains und deren Anwendungsgebiete zu geben. Die Potenziale der Technologie für unterschiedliche Sektoren sollten aufgezeigt und darauf aufbauend gesellschaftliche und politische Implikationen detailliert analysiert werden. Als Ausgangspunkt könnte eine aktuelle Veröffentlichung des UK Government Office for Science (2016) dienen. Auf dieser Basis könnten Optionen für den Umgang mit Blockchains in verschiedenen Anwendungskontexten erarbeitet werden.

Zur ersten Vertiefung des Themas wäre es auch möglich, zunächst ein sondierendes Fachgespräch mit Experten der IT-Branche sowie mit Vertretern aus den Bereichen des Banken- und Versicherungswesens und der Rechtswissenschaften zu den Anwendungsperspektiven und Herausforderungen der Blockchaintechnologie im Bundestag durchzuführen (im Format ähnlich wie das Fachgespräch im Februar 2016 zum 3-D-Druck). Die inhaltliche Vorbereitung, die Ergebnisse des Fachgesprächs sowie konzeptionelle Überlegungen für weiterführende Untersuchungen würden dann in einer Kurzstudie aufbereitet.

Literatur

Bartlett, J. (2015): The dark net. Inside the digital underworld. New York

BTC-Echo: Wie funktioniert Bitcoin Mining. http://www.btc-echo.de/wie-kann-ich-bitcoins-minen/ (26.4.2016)

Bundesverband deutscher Banken e. V. (2015): Antworten des Bankenverbands auf die Fragen des Ausschusses Digitale Agenda für das Fachgespräch »Digitalisierung der Finanzbranche«. Berlin

Cabinet Office; Hancock, M.; Government Digital Service (2016): Government explores blockchain technology to improve public services. The government has outlined ways the state could use blockchain technology to track payments and provide public services. 28.4. https://www.gov.uk/government/news/government-explores-blockchain-technology-to-improve-public-services (16.6.2016)

Casey, M.; Vigna, P. (2015): Cryptocurrency. Wie virtuelles Geld unsere Gesellschaft verändert. Berlin

Cassano, J. (2014): What Are Smart Contracts? Cryptocurrency's Killer App. www.fastcompany.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app (27.4.2016)

CoinMarketCap (2016): Crypto-Currency Market Capitalizations. http://coinmarketcap.com/ (27.4.2016)

Conrad, P. (2013): Bitcoin – Perspektive oder Risiko? Berlin

Cox, J. (2014): Silk Road 2.0 Was Just Shut Down by the FBI. 6.11. http://motherboard.vice.com/read/silk-road-2-has-been-seized-by-the-fbi (28.6.2016)
Dapp, T.–F. (2016): Heute schon mit Blockchain experimentiert? http://dbresearch.de/servlet/reweb2.ReWEB;RWSESSIONID=E961FDA49ADC4FF86292E1474DB2D822.srv-tc2-dbr-de?rwsite=DBR_INTERNET_DE-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000394657 (25.4.2016)
Dapp, T.–F.; Karollus, A. (2015): Blockchain – Angriff ist wahrscheinlich die beste Verteidigung. www.dbresearch.de/servlet/reweb2.ReWEB?rwsite=DBR_INTERNET_DE-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000358989 (25.4.2016)
Die Zeit (2013): FBI schließt virtuellen Schwarzmarkt Silk Road. 3.10. www.zeit.de/digital/internet/2013-10/fbi-silk-road-ulbricht (28.6.2016)
Dingledine, R.; Mathewson, N. (2002): The Onion Router. https://www.torproject.org/ (26.4.2016)
D'Orazio, D. (2015): Former Mt. Gox CEO arrested on claims of stolen bitcoins. 1.8. www.theverge.com/2015/8/1/9083989/mt-gox-ceo-arrested-in-tokyo/in/5297313 (29.6.2016)
EtherCasts (2016): State of the Dapps using Ethereum. http://dapps.ethercasts.com/ (27.4.2016)
finews.ch (2015): Die Banken und das Blockchain-Dilemma. 20.8. www.finews.ch/news/banken/19024-banken-ubs-blockchain-auflistung-fidor-citi-goldman-sachs-anz-bnp-paribas-abn-amro-rabobank-societe-generale-oliver-bussmann (1.6.2016)
Government Office for Science (2016): Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser. London
Grollmann, D. (2016): Zukunftstechnik Blockchain: Wie Verträge smart und Banken arm werden. In: iBusiness Executive Summary (08), S. 14–15
Gundlach, J. (2015): Vertrauen programmiert. www.zeit.de/2015/46/bitcoin-revolution-waehrung-geschaefte-bezahlsystem (25.4.2016)
He, D.; Habermeier, K.; Leckow, R.; Haksar, V., Almeida, Y.; Kashima, M.; Kyriakos-Saad, N.; Oura, H.; Sedik, T.S.; Stetsenko, N.; Verdugo-Yepes, C. (2016): Virtual Currencies and Beyond. Initial Consideration. International Monetary Fund, o.O.
Kastrenakes, J. (2014): Mt. Gox finds over $100 million of customers' missing bitcoins. 21.3. www.theverge.com/2014/3/21/5532876/mt-gox-200000-missing-bitcoins-found-in-old-wallet/in/5297313 (29.6.2014)
Koning, J.P. (2014): Fedcoin. 19.10. http://jpkoning.blogspot.de/2014/10/fedcoin.html (1.6.2016)
Locker, T. (2016): Auf der Ethereum-Blockchain sind gerade 53 Millionen Dollar verschwunden. 20.6. http://motherboard.vice.com/de/read/ein-typ-hat-gerade-53-millionen-dollar-von-der-ethereum-blockchain-stibitzt (28.6.2016)
Martin, W. (2014): Black Market Cryptocurrencies: The rise of bitcoin alternatives that offer true anonymity.
Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (21.4.2016)
Platzer, J. (2014): Bitcoin – kurz & gut. Banking ohne Banken. CA 95472

Schulz, B. (2016a): Das ärgert Betrüger. Weniger Verbrechen, weniger Kosten, weniger Arbeit: Die Technologie hinter der Digitalwährung Bitcoin könnte die Finanzwelt von Grund auf verändern – und sogar den Handel mit Diamanten oder Kunst. www.zeit.de/2016/03/blockchain-bitcoin-digital-sicherheit-anonymitaet/komplettansicht (28.1.2016)
Schulz, B. (2016b): Spuren des Geldes. Die Digitalwährung Bitcoin hat die Blockchain bekannt gemacht – und zeigt gleichzeitig ihre Grenzen auf. www.zeit.de/2016/03/bitcoins-digitale-waehrung-blockchain (25.4.2016)
Slock.it UG (2016): Slock.it. Slock.it brings the benefits of the Blockchain – transparency, security and auditablity – to real-world objects. https://slock.it/ (27.4.2016)
Storm, A. (2015): App statt Banken. Immer häufiger kehren Privatkunden Geldinstituten den Rücken. Sie nutzen Angebote innovativer neuer Firmen. Die Traditionshäuser fürchten um ihr Geschäft – und reagieren. 28.5. www.zeit.de/2015/20/fintech-banken-konkurrenz/komplettansicht (25.4.2016)
Studer, B. (2010): Netzwerkmanagement und Netzwerksicherheit. Ein Kompaktkurs für Praxis und Lehre. Zürich
Swan, M. (2015): Blockchain. Blueprint for a new economy. Peking
Swanson, T. (2014): Blockchain 2.0 – Let a Thousand Chains Blossom. https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom (26.4.2016)
Szabo, N. (1994): Smart Contracts. http://szabo.best.vwh.net/smart.contracts.html (27.4.2016)
Weiss, M. (2014): Die Bitcoin-Blockchain könnte die Finanz- und Tech-Branche umkrempeln. https://www.wired.de/collection/tech/die-bitcoin-blockchain-konnte-die-finanz-und-tech-branche-umkrempeln (25.4.2016)
Wetzel, K. (2016): Blockchain. Im Fieber. www.sueddeutsche.de/wirtschaft/blockchain-im-fieber-1.2908084 (27.4.2016)

BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG

KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)

Neue Schönhauser Straße 10
10178 Berlin

Tel. +49 30 28491-0
Fax +49 30 28491-119

buero@tab-beim-bundestag.de
www.tab-beim-bundestag.de