Blockchain #Banking

Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien

www.bitkom.org

Osborne Clarke

NTT DATA
Global IT Innovator

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Marco Liesenjohann | Bitkom e. V.
T 030 27576-207 | m.liesenjohann@bitkom.org

Verantwortliches Bitkom-Gremium

AK SEPA, Instant Payments & Crypto Currencies

Projektleitung

Marco Liesenjohann | Bitkom e. V. (Projektkoordinator)
Benjamin Matten | NTT DATA Deutschland GmbH
Dr. Matthias Terlau | Osborne Clarke

In Zusammenarbeit mit

NTT DATA Deutschland GmbH
Martin Brugger | Business Development Executive
Königsberger Straße 1 | 60487 Frankfurt a. Main
T 069 97261-213 | martin.brugger@nttdata.com

Osborne Clarke
Dr. Matthias Terlau | Rechtsanwalt
Innere Kanalstraße 15 | 50823 Köln
T 0221 5108 4088 | matthias.terlau@osborneclarke.com

Titelbild

© alptraum – istockphoto.com

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

1 Einführung

In den letzten 12 Monaten sind die Artikel und Berichte über die »Blockchain« nahezu exponentiell in die Höhe geschnellt. Was verbirgt sich inhaltlich hinter dem Begriff Blockchain oder dem häufig – wenn auch irreführend – synonym verwendeten »Distributed Ledger«?

Glaubt man den zahlreichen Berichten, wohnt der Blockchain-Technologie das Potential inne, vor allem im Finanzsektor erhebliche Veränderungen herbeizuführen. Insbesondere im Bankenbereich haben viele Prozesse ihr Erbe aus der manuellen Welt mit ins digitale Zeitalter getragen. Banken haben zwar nach und nach digitale Technologien eingeführt, um ihre Prozesse zu optimieren, konzentrierten sich jedoch vorwiegend auf die Automatisierung einzelner Prozessschritte. Die grundsätzlichen Abläufe, beispielsweise bei bankübergreifenden Transaktionen, blieben weitgehend unverändert und bedürfen nach wie vor vieler Intermediationsleistungen.[1]

Kryptowährungen, wie z. B. Bitcoin, haben die Eignung von Distributed Ledger Technologien für den Einsatz im Finanzsektor nicht nur praktisch bewiesen, sondern auch die ersten Schwachstellen der Technologie hinsichtlich Regulierung, Skalierbarkeit, Geschwindigkeit und Sicherheit in der Peripherie aufgezeigt. Die Analyse der Vorfälle um Mt. Gox, dem 2010 bis Anfang 2014 größten Handelsplatz für Bitcoin, deckte die Verwundbarkeit der Blockchain-Architektur im Zusammenspiel mit Sicherheitslücken von Wallet-Lösungen auf; dennoch wurde der Blockchain-Technologie selbst die Einschätzung zuteil, dem hohen Anspruch an Sicherheit und Nachvollziehbarkeit zu genügen. Deswegen sind die bisher durch große Anstrengungen in der Regulierung erreichten Fortschritte nicht zuletzt hinsichtlich Geldwäsche und Fraud Prevention auch bei dieser neuen Technologie anzuwenden und wo notwendig technologiespezifisch anzupassen. Die denkbaren Einsatzmöglichkeiten der Distributed Ledger Technologie über Kryptowährungen hinaus haben die Aufmerksamkeit einer weitaus größeren Interessensgemeinschaft geweckt.

Im Vergleich zu den vorherrschenden Systemarchitekturen handelt es sich bei der Blockchain-Technologie um einen Ansatz, der einen radikalen Konzeptwechsel mit sich bringt und Transaktionen unmittelbar zwischen den Geschäftspartnern unter Verzicht auf viele der heute noch notwendigen Intermediärsleistungen ermöglicht. Damit eröffnen sich einerseits Effizienzsteigerungsmöglichkeiten und andererseits Raum für Innovationen.[1] Im Folgenden möchten wir betrachten, warum dieser Technologie ein derartiges Potential zugetraut wird. Dafür ist es notwendig die Grundzüge hinter diesem Konzept zu verstehen.

Analog zu einigen technischen Innovationen der letzten Jahre existiert auch bei der Distributed Ledger Technologie (DLT) eine technische Lösung für ein technisches Problem mit interessanten Implikationen für fachliche Anwendungsfälle.

Unabhängig davon, dass diese Technologie hohe Relevanz für unterschiedlichste Industriezweige hat, fokussiert sich diese Abhandlung auf die Finanzindustrie – aufgrund der Bitcoin-Historie auch als DLT-Ursprungsindustrie zu bezeichnen. Bei der Anwendung der aktuell vorhande-

1 Prof. Rossbach.

nen Protokolle und Technologien sind in dieser höchstregulierten Branche deutlich größere Herausforderungen zu bewältigen als in anderen Wirtschaftsbranchen.

Bitkom möchte dem Leser des Leitfadens eine grundlegende und verständliche Einführung in die Blockchain-Systematik zur Hand geben und auf diese Weise auch mit vielen Missverständnissen aufräumen. Der Leitfaden gibt einen Überblick über die Historie und die Funktionsweise der Blockchain. Weitergehend werden gängige Anwendungsfälle und deren Qualifizierung vorgestellt, sowie rechtliche Fragestellungen und Auswirkungen auf die Finanzwirtschaft untersucht.

1.1 Einordnung in Wirtschaft, Wissenschaft und Politik

Blockchain ist der Begriff mit der zweithöchsten Anzahl an Nennungen in der aktuellen Deep-Shifts-Analyse des World Economic Forums.[2] Im Jahr 2015 sind mehr als eine Milliarde Dollar in Bitcoin-Technologie-Start-ups investiert worden[3] – und davon knapp die Hälfte in Unternehmen, Geschäftsmodelle und Technologieweiterentwicklungen, die sich ausschließlich mit der Blockchain befassen.[4] Ein Jahr zuvor hatte die Bank of England in einer Bekanntmachung zur Weiterentwicklung von Zahlungsverfahren auf die Bedeutung der »Distributed Ledger Technology« im Sinne einer dezentralen Kontoführungstechnologie hingewiesen.[5]

In der Bankenbranche hat das Thema Blockchain das derzeit größte Momentum. Die Deutsche Bank Research teilte Anfang 2016 mit, dass die Blockchain eine Finanztechnologie mit solch disruptivem Potential sei, einen Paradigmenwechsel im Finanzsystem herbeizuführen. Für Lawrence Wintermeyer, Chef von Innovate Finance, einem Londoner FinTech-Verband, ist die Blockchain-Technologie gar die größte Erfindung seit der Einführung des Internets.[6] Der CIO der schweizerischen Großbank UBS, Oliver Bussmann, erwartet erste vertrauenswürdige Produkte auf Blockchain-Basis in der Mitte des Jahres 2016 und betont das starke Engagement für entsprechende Technologieentwicklungen durch den CEO.[7]

Die großen Banken engagieren sich dementsprechend in zahlreichen Initiativen und Kollaborationen zur Weiterentwicklung der Blockchain-Technologie: das New Yorker Start-up R3 versam-

2 World Economic Forum, Survey report (September 2015), »Deep Shift | Technology Tipping Points and Societal Impact«. ↗ http ://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

3 Jose Pagliery, CNN Money. ↗ http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested

4 Bettina Schulz, zeit.de
↗ http://www.zeit.de/2016/03/blockchain-bitcoin-digital-sicherheit-anonymitaet

5 Robleh Ali, John Barrdear, et al. »Innovations in payment technologies and the emergence of digital currencies«. ↗ http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalwährungenbitcoin1.pdf

6 Bettina Schulz, zeit.de
↗ http://www.zeit.de/2016/03/blockchain-bitcoin-digital-sicherheit-anonymitaet

7 Clint Boulton, cio.com. ↗ http://www.cio.com/article/2972588/cio-role/cio-says-blockchain-will-heavily-impact-financial-services.html

melt ein Konsortium zahlreicher Banken hinter sich (darunter HSBC, J.P. Morgan, Banco Santander, Deutsche Bank und Commerzbank).[8] Im »Hyperledger« genannten Projekt der Linux Foundation finden sich Börsenbetreiber mit Unternehmen wie Intel, Fujitsu, IBM und NTT DATA zusammen.[9] Die Beteiligung der zuletzt genannten Gruppe von Unternehmen und die ersten Initiativen zur Blockchain bei Mischkonzern Bosch deuten darauf hin,[10] dass die Blockchain auch Relevanz für andere Branchen und Industrien besitzt.

Das Meinungsbild zur Blockchain in der Wissenschaft ist vielfältig und ausdifferenziert: Stephen G. Cecchetti, Professor an der Brandeis International Business School, meint, dass die vorhergesagten Effizienzgewinne durch Einsatz von Blockchain-Technologien gegenüber dem status quo in der Finanzindustrie kaum erwähnenswert seien.[11] Professor Roßbach von der Frankfurt School of Finance and Management zeigt sich vom technischen Konzept der Blockchain überzeugt, denn der Bitcoin habe bewiesen, dass die Protokolle sicher seien.[12] Die Rechtswissenschaftler De Filippi und Wright diskutieren, als Reaktion auf die absehbaren Auswirkungen der Blockchain-Technologie auf den rechtlichen Raum, eine »Lex Kryptographia«.[13]

Und auch in der Politik erfährt die Technologie Blockchain große Aufmerksamkeit: der leitende wissenschaftliche Berater der britischen Regierung, Sir Mark Walport, hat Anfang 2016 einen ausführlichen Bericht[14] zu den Chancen der Blockchain-Technologie der Regierung des Vereinigten Königreichs vorgestellt.[15] Ende März 2016 fand sich der Begriff Blockchain erstmals in einem Gesetz aus dem Haus des französischen Finanzministeriums wieder.[16]

Die Blockchain, als zentrale Innovation der ersten erfolgreichen Kryptowährung, wandelt sich damit zu einer eigenständigen technologischen Innovation, die vollkommen unabhängig von Bitcoin wahrgenommen wird.

---

8 Oscar Williams-Grut, Business Insider. ↗ http://www.businessinsider.de/blockchain-r3-membership-hits-42-as-it-looks-to-non-banks-2015-12?_ga=1.115313543.1402963512.1454922306?r=UK&IR=T

9 Jennifer Cloer, The Linux Foundation News. ↗ https://www.hyperledger.org/news/announcement/2016/02/hyperledger-project-announces-30-founding-members

10 Markus Weinberger, Bosch Connected World Blog. ↗ http://blog.bosch-si.com/categories/business-models/2015/06/bitcoin-enabler-for-the-iot

11 Stephen G. Cecchetti, Kermit Schoenholtz, huffingtionpost.com ↗ http://www.huffingtonpost.com/stephen-g-cecchetti/virtual-frenzies-bitcoin_b_8228444.html

12 Tim Kanning, Christian Siedenbiedel, faz.net. ↗ http://www.faz.net/aktuell/finanzen/digital-bezahlen/blockchain-heisst-die-technik-hinter-der-internetwaehrung-bitcoin-14063245.html

13 Aaron Wright, Primavera De Filippi, »Decentralized Blockchain technology and the rise of Lex Cryptographia«. ↗ https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

14 British Government Office of Science, »Distributed Ledger Technology: Beyond Block Chain«. ↗ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

15 John Naughton, theguardian.com. ↗ http://www.theguardian.com/commentisfree/2016/jan/24/blockchain-bitcoin-technology-most-important-tech-invention-of-our-age-sir-mark-walport

16 Enguérand R., Benjamin F., Le Figaro. ↗ http://www.lefigaro.fr/secteur/high-tech/2016/03/24/32001-20160324ARTFIG00317-macron-amenage-la-loi-pour-tester-la-blockchain-sur-la-finance.php

Mit der massiven medialen Präsenz des Themas geht eine Verwendung von Begriffen einher, die selten erklärt werden. Daraus resultieren einige Missverständnisse und eine missbräuchliche Verwendung von Terminologie.

1.2 Begriffliche Abgrenzung

Die am häufigsten verwendeten Begriffe werden im Folgenden anhand eines Schichtenmodells erklärt.

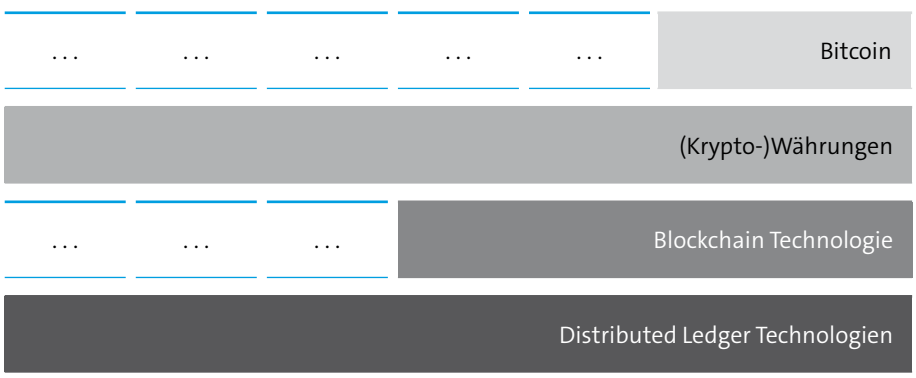


Abbildung 1: Begriffe im Blockchain-Universum – Schichtenmodell

Distributed Ledger

Der Distributed Ledger bildet die Basis des Schichtenmodells. Er ist im Grunde genommen ein klassisches Bestandsbuch, das über einen Mechanismus verfügt, es auf alle teilnehmenden Parteien zu verteilen. Distributed Ledger existieren bereits seit längerer Zeit und sind meist auf der technischen Basis einer verteilten Datenbank mit einer Logik auf Programm- oder Datenbankseite versehen, die aus der reinen Datenbank ein Bestandsbuch macht.

»Distributed Ledger Technologie« wird zunehmend synonym zum bisherigen Gebrauch von »Blockchain« genutzt, um die Entwicklungen nach dem Bitcoin und den Kryptowährungen von eben diesen begrifflich abzugrenzen.

Blockchain

Die Blockchain ist eine Form, einen Distributed Ledger zu organisieren und zu implementieren. Auf die technische Implementierung der Blockchain wird in den folgenden Kapiteln näher eingegangen; zur Begriffsbestimmung seien hier die grundlegenden Eigenschaften aufgezählt, die der Blockchain in den letzten Jahren die steigende Aufmerksamkeit in Medien und bei Analysten ermöglicht haben:

- **Dezentralisiert:** Es gibt keine zentrale Instanz, die den Distributed Ledger verwaltet, jeder Teilnehmer am Netzwerk ist gleichberechtigt und es gibt einen Mechanismus, um den Konsens über den Zustand des Bestandsbuchs über alle Teilnehmer herzustellen. Teilnehmer werden als Nodes bezeichnet, da sie die Knotenpunkte des Netzwerkes darstellen. Die Verteilung der Nodes erlaubt eine Skalierung auf eine sehr große Anzahl von Nodes.
- **Peer-to-Peer:** Die Gleichberechtigung aller Teilnehmer ermöglicht Transaktionen zwischen Nodes, ohne eine zentrale Instanz zu nutzen. Es werden nicht mehr Nodes benötigt als die zwei, zwischen denen eine atomare Transaktion durchgeführt werden soll. Intermediäre, die die Korrektheit der Transaktion und deren tatsächliche Ausführung garantieren, werden nicht benötigt.
- **Transparenz und Anonymität:** Alle Transaktionen werden für alle Teilnehmer des Netzwerks veröffentlicht. In den öffentlich zugänglichen Blockchain-Implementierungen ist neben dieser Transparenz auch die Anonymität der handelnden Nodes realisiert. Für jede Transaktion kann ein Teilnehmer eine neue Adresse, unter der er im Netzwerk zu erreichen ist, generieren. So werden effektiv eine Nachvollziehbarkeit von Transaktionen und Identifizierung der Teilnehmer erreicht.
- **Trust:** Die Blockchain implementiert ein Bestandsbuch, das nur durch Transaktionen verändert werden kann, zurückliegende Blöcke, die eine Historie aller Transaktionen darstellen, können nicht mehr verändert werden. Das Verfahren, mit dem Transaktionen durchgeführt werden können, garantiert die Sicherheit der Abwicklung. Ein Übertrag eines Assets von einem Teilnehmer auf einen anderen kann nur durchgeführt werden, wenn der »Veräußerer« auch über das Asset verfügt. Wenn die Transaktion bestätigt wird, ist das Asset sicher übertragen und es ist nicht möglich, diese Transaktion zu kopieren (das sogenannte »Double Spending«[17]) und damit erneut durchzuführen oder sie nachträglich zu verändern. Durch diese Eigenschaften wird ein Handel zwischen Parteien ermöglicht, ohne dass diese sich gegenseitig vertrauen müssen oder eine unparteiische Stelle die korrekte Abwicklung sicherstellt.

Kryptowährungen

Mit der Blockchain als Basistechnologie lassen sich darauf aufbauende komplexe Systeme, wie z. B. Währungen abbilden. Erstmals beschrieben wurde die Blockchain-Technologie im Jahre 2008 im Zusammenhang mit einer Kryptowährung, dem Bitcoin, in einer Veröffentlichung eines Autors unter dem Pseudonym Satoshi Nakamoto.[18] Die Blockchain ist somit ein »Nebenprodukt« einer technischen Plattform, die eine kryptographische Währung erschuf und gleichzeitig ein System implementierte, um diese Währung zu nutzen und zu handeln.

Neben dem Bitcoin existiert eine Reihe weiterer Kryptowährungen, die sich zum Teil der dem Bitcoin zugrunde liegenden öffentlichen Blockchain bedienen. Genannt seien hier z. B. Litecoin oder Dogecoin. Es existieren darüber hinaus Kryptowährungen, die eigene Blockchains zur Basis

17 Michael Nielsen, Data Driven Intelligence.
↗ http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works

18 Bitcoin.org »Bitcoin: A Peer-to-peer Electronic Cash System«. ↗ https://bitcoin.org/bitcoin.pdf

haben – zum Teil auf einer komplett eigenen technischen Implementierung. Vertreter hierfür sind z. B. Ethereum und Ripple.

Bitcoin

Der Bitcoin ist die Kryptowährungseinheit, die auf der ursprünglichen Blockchain gehandelt wird (weiteres dazu siehe Kapitel 4.1).

2 Funktionsweise der Blockchain

2 Funktionsweise der Blockchain

Einige der Eigenschaften, die zur Implementierung des Bitcoins notwendig waren, finden sich auch in der technischen Implementierung des Protokolls wieder. Die zentrale Idee der Blockchain ist das sichere Übertragen von digitalen Assets zwischen Parteien, im Falle von Ethereum oder Bitcoin z. B. in Form einer Währung. Dies geschieht mit einer Distributed Ledger Implementierung, die in der Blockchain auf eine revolutionär neue Art umgesetzt wurde.

2.1 Transaktionen und Blöcke

In der Blockchain werden digitale Ereignisse – Transaktionen, die den Ledger verändern – chronologisch geordnet eingetragen. Diese Transaktionen werden im gesamten Netzwerk publiziert und zu Blöcken zusammengefasst. Hierbei werden die Transaktionen geprüft – z. B. darauf, ob die digitale Signatur des Initiators der Transaktion mit der Adresse übereinstimmt. Der jeweils aktuelle Block wird mit einem Hash-Algorithmus vor Veränderungen geschützt und dabei mit dem Hash-Wert des vorherigen Blocks verbunden. So entsteht eine Kette, die namensgebende Blockchain, bei der Blöcke nicht mehr verändert werden können. Die Manipulation eines Blocks zieht je nach Art der Manipulation eine Veränderung von Blöcken in der Vergangenheit nach sich, zumindest aber vom manipulierten Block bis zum aktuellen Block. Der hierfür notwendige Aufwand ist exorbitant groß, da erst durch die erneute kryptographische Absicherung von allen folgenden Blöcken genügend Knoten im Netzwerk von der Richtigkeit des manipulierten Blocks überzeugt werden könnten. Der neu entstandene und geprüfte Block wird an alle Teilnehmer des Netzwerkes verteilt. Jeder Teilnehmer hat hierdurch jederzeit eine Kopie der aktuell gültigen Blockchain.

Dieses Verfahren der blockweisen Prüfung, Absicherung und Verkettung verleiht der Blockchain die Eigenschaft, die sie in den Augen vieler so besonders und revolutionär macht: Die Prüfung eines Blocks wird nicht von einer zentralen, korrumpierbaren Vertrauensstelle durchgeführt, sondern wird, wie die gesamte Transaktionsdokumentation, parallel von sehr vielen Akteuren realisiert. Dieses Prinzip des Distributed Consensus macht die Konsistenzprüfung der Transaktionen vollkommen unabhängig von einer einzelnen vertrauenswürdigen Instanz. Für die Herstellung des Konsenses gibt es verschiedene Verfahren, einige sind im folgenden Kapitel aufgeführt.

2.2 Mining, Blockbildung und Konsensmechanismen

In der größten öffentlichen Blockchain, der Bitcoin Blockchain, wird der Vorgang der Blockbildung als »Mining« bezeichnet. Dieser Begriff hat sich auch bei anderen Implementierungen durchgesetzt und wird dort synonym verwendet.

Für die Herstellung des Konsenses in Distributed Ledgern gibt es mehrere Ansätze. Einige sind bereits implementiert und werden in öffentlichen und privaten Blockchains (mehr dazu im nächsten Kapitel) verwendet, andere sind noch im Stadium theoretischer Untersuchung oder Proof of Concepts.

2.2.1 Proof of Work

Die Art und Weise wie das »Gegenlesen« des Ledgers funktioniert, wird erstmals im Bitcoin Whitepaper unter dem Namen »Proof-of-Work (PoW) chain« erläutert. Ein PoW ist ein mathematisches Rätsel, das eine starke Asymmetrie zwischen dem Aufwand zum Erzeugen einer zulässigen Lösung gegenüber dem Aufwand zum Überprüfen einer bereits gefundenen Lösung aufweist. Auf z. B. die Bitcoin-Blockchain übertragen, bedeutet das: Jeder der prüfenden Akteure investiert sehr viel Rechenkapazität, um einen Block im Zuge des Prüfens an die Kette bestehender Blöcke anhängen zu dürfen. Für alle anderen Akteure im Netzwerk ist nach erfolgtem Anhängen des Blocks jedoch augenblicklich klar, ob der neu angehängte Block die Voraussetzung zum Anhängen erfüllt. Um Manipulationen vorzubeugen wird der Node, der den Block validiert, mit einem Zufallsalgorithmus ausgewählt.

Die treibende Kraft, die das PoW-Konzept am Laufen hält, ist eine Entlohnung, die den Aufwand des prüfenden Akteurs auf lange Sicht leicht überkompensiert (in der Blockchain-Technologie-Variante des Bitcoins sind es Bitcoins selbst).[19] Der Aufwand ist Rechenleistung mal Zeit und wird letztlich durch die Kostenstelle für den Energieverbrauch repräsentiert. Der sich anpassende Schwierigkeitsgrad des zu lösenden PoWs sorgt dafür, dass eine nachträgliche Änderung eines früheren Blocks beliebig aufwändig wird.[20] Eine rückwirkende Manipulation, in Form des Ersetzens eines bereits verankerten Blocks durch einen betrügerischen Akteur, ist damit praktisch ausgeschlossen – es sei denn, die Logik einer Side- bzw. Altchain wird anfänglich so konfiguriert, dass ein befugter Administrator Blöcke und/oder Transaktionen nachträglich ändern darf.

Durch diese Art der technischen Implementierung wird erreicht, dass die Gesamtheit der Akteure die Blöcke neutral und rein finanziell motiviert, d. h. unabhängig von den Blockinhalten und im Sinne der Regeln des Netzwerks, prüft. Akteure mit betrügerischer Absicht können zwar jederzeit Blöcke mit manipulierten Transaktionen prüfen und an ihr Ende der Blockchain anhängen, aber das »distributed consensus«-Prinzip wird immer dafür Sorge tragen, dass sich letzten Endes eine manipulationsfreie Blockchain realisiert.

19 Bitcoin.org. ↗ https://bitcoin.org/de/faq

20 Simon Barber et al., »Bitter to Better — How to Make Bitcoin a Better Currency«. ↗ http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf

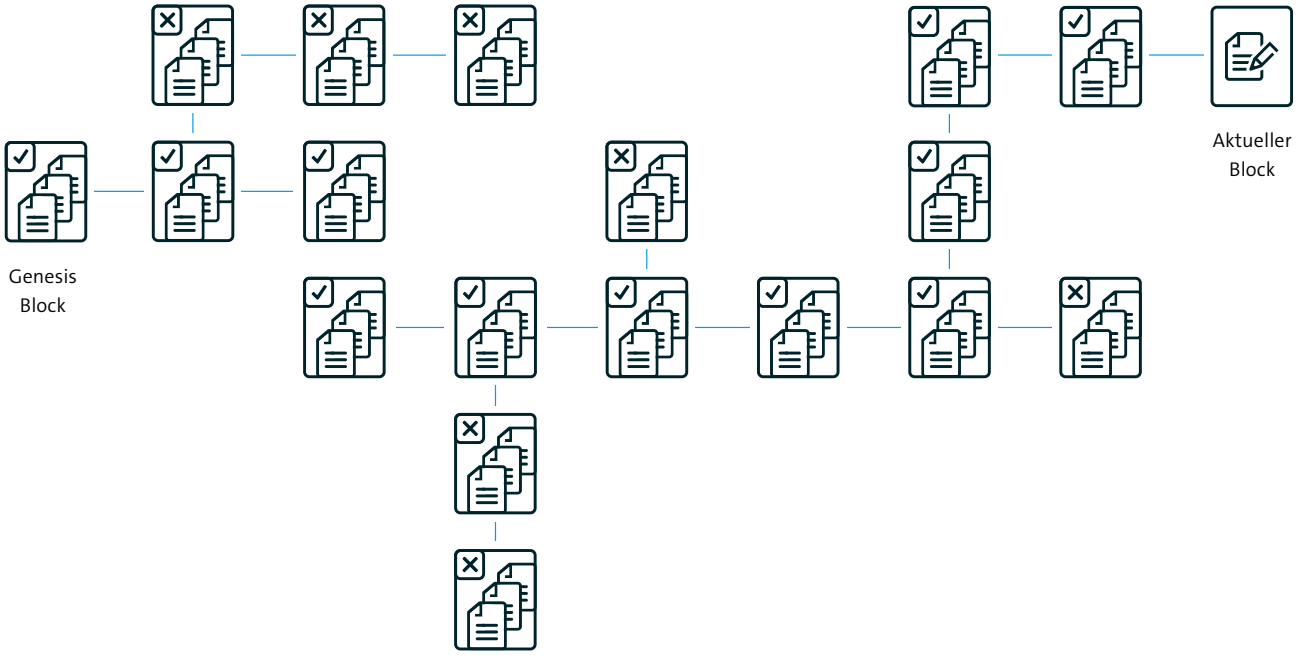


Abbildung 2: Schematische Ansicht der Blockchain

In einem gewissen Zeitfenster ist damit das Ende der Blockchain diffus. Vorstellen kann man sich das wie folgt: Das Ende der Blockchain ähnelt den sich verästelnden Armen, wenn sich ein Wasserstrom über einer zerklüfteten Fläche ausbreitet – die versiegenden Nebenströme stellen die manipulierten Blockchain-Varianten dar (mit einem Kreuz markierte Blöcke in Abbildung 2), der sich herausbildende Hauptstrom ist die mehrheitsgeprüfte, fehlerfreie Blockchain (angedeutet durch die mit einem Haken markierten Blöcke in Abbildung 2). Aus der Rückschau und aus technischer Sicht stellt sich stets die längste Blockaneinanderreihung als manipulationsfreie Blockchain heraus. In sie ist die meiste Rechenleistung investiert worden. Dieses Prinzip erweist sich als robust und nicht zu kompromittieren, solange eine wesentliche Bedingung erfüllt ist: Mehr als 50 Prozent der Rechenleistung im Netzwerk[21] wird durch Prüfer ohne manipulative Absichten bereitgestellt.

In öffentlichen Blockchains ist der PoW der derzeit am stärksten vertretene Konsensmechanismus. Ausgelegt auf den Bitcoin wurde er entworfen, um den Anforderungen einer öffentlichen Blockchain gerecht zu werden.

21 Mike Gault, recode.net
↗ https://www.linkedin.com/pulse/forget-bitcoin-what-blockchain-why-should-you-care-source-ben-aissa

2.2.2 Proof of Stake

Als eine Alternative zum PoW ist der Proof of Stake (PoS) entwickelt worden. Der PoS basiert auf dem Beweis, dass der validierende Knoten eines Blocks über ein entsprechendes Engagement in der der Blockchain zugrundeliegenden Kryptowährung verfügt. Er würde sich praktisch selbst schaden, wenn er die Transaktionen manipuliert. Neben diesem Grundprinzip werden Manipulationen noch über weitere Mechanismen verhindert. Der PoS wurde für öffentliche Blockchains untersucht, hat sich aber als sehr herausfordernd in der Realisierung herausgestellt. So hat sich z. B. das Ethereum Projekt gegen eine Implementierung des PoS entschieden.

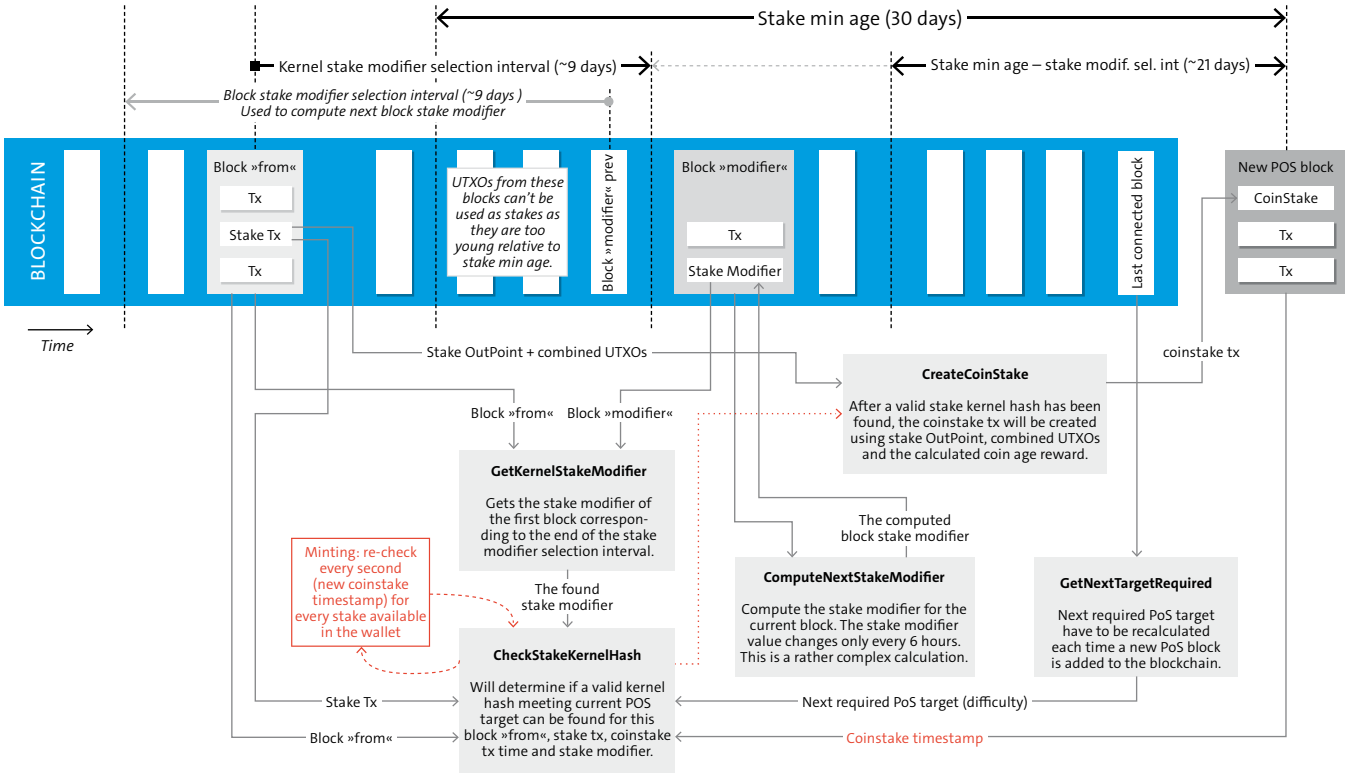


Abbildung 3: Proof of Stake in der PeerCoin Implementierung[22]

Der PoS wurde 2011 zum ersten Mal in der Kryptowährung PeerCoin realisiert. Einer der wesentlichen Vorteile gegenüber dem PoW ist die Effizienz des Mining-Vorgangs. Eine wesentliche Kritik am PoS ist, dass wesentlich mehr Vektoren für Angriffe existieren. So ist z. B. Double Spending in PoS leichter möglich als in PoW-Systemen und macht eine weitergehende Absicherung erforderlich.

22 Mably, PeerCoin. ↗ http://ppcsuite.github.io/images/peercoin-pos-diagram.html

2.2.3 Weitere Konsensmechanismen

Neben den zuvor geschilderten Methoden gibt es eine Vielzahl von Abwandlungen oder exotischen Konzepten wie Proof of Burn (kostenintensives Mining entfällt, wenn ein den Kosten entsprechender Betrag vernichtet wird) oder der komplette Verzicht auf einen Proof-of-Mechanismus, wie z. B. in einigen Varianten des Hyperledger implementiert. Entscheidend ist letztlich, dass ein Konsensmechanismus zum Zweck der Blockchain kompatibel gewählt wird.

2.3 Öffentliche und private/konsortiale Blockchains

Als öffentliche Blockchains werden Netzwerke bezeichnet, bei denen es keine oder sehr geringe Hürden für den Zugang und zur Nutzung des Netzwerks gibt. Das Netzwerk wird auch nicht durch einen offiziellen »Betreiber« unterhalten, der zentrale Elemente der Infrastruktur bereitstellt. Die derzeit größten öffentlichen Netzwerke wie die Ethereum-Blockchain und die ursprüngliche Bitcoin-Blockchain verzichten zusätzlich auf eine echte Identifizierung der Teilnehmer. Dies entspricht der Philosophie und dem Business Case der offenen Kryptowährungen, möglichst jedem die Nutzung der Währung unter Wahrung der Anonymität zu ermöglichen.

Im Zuge der Weiterentwicklung der Technologie und einer breiteren Basis von Anwendern gibt es weitere Nutzungsszenarien, die sich grundlegend von denen der öffentlichen Kryptowährungs-Blockchains unterscheiden. Netzwerke, wie z. B. der Utility Settlement Coin[23], der in einer Kooperation zwischen der UBS, BNY Mellon, Deutsche Bank, Santander und ICAB in Zusammenarbeit mit Clearmatics entwickelt wird, dienen der Abwicklung von Zahlungen in institutionellen Finanzmärkten. Für diesen und ähnliche Anwendungsfälle sind öffentliche Netzwerke nicht sinnvoll. Diese Netzwerke werden zumeist von einem einzelnen (privat) oder einer Gruppe (konsortial) betrieben und die Eigenschaftsausprägung der Blockchain, wie z. B. die Identifizierung von Teilnehmern oder der Konsensmechanismus ist anwendungsspezifisch. Die Herausforderung bei privaten Blockchains besteht im Finden des richtigen Business Cases, des Erreichens einer Anzahl von Teilnehmern, die den Einsatz der Technologie rechtfertigt. Ein prominentes Beispiel für ein konsortiales Netzwerk ist das Netzwerk von Ripple.

23 Diverse Autoren. ↗ https://www.ubs.com/microsites/blockchain-report/en/home.html

3 Das Blockchain Ökosystem im Kontext seiner Stakeholder

3 Das Blockchain Ökosystem im Kontext seiner Stakeholder

Die Interessenslage entlang der Wertschöpfung mittels dieser neuen Technologie ist sowohl auf Anwender- und Zuliefererseite als auch auf kompetitiver Seite bzw. bei sonstigen einflussnehmenden Gruppen sehr heterogen.

Die einzelnen Elemente eines Distributed Ledger Wertschöpfungsnetzwerks, hier im speziellen basierend auf der Blockchain-Technologie, werden von unterschiedlichen Marktteilnehmern realisiert, weiterentwickelt und letztendlich operational monetarisiert. Neben einer Vielzahl an Open Source Projekten zu einzelnen Aspekten gibt es zahlreiche FinTech-Unternehmen, große Softwarehäuser und »klassische« Unternehmen der Finanzindustrie, die Teile der Blockchain Wertschöpfungskette adressieren.

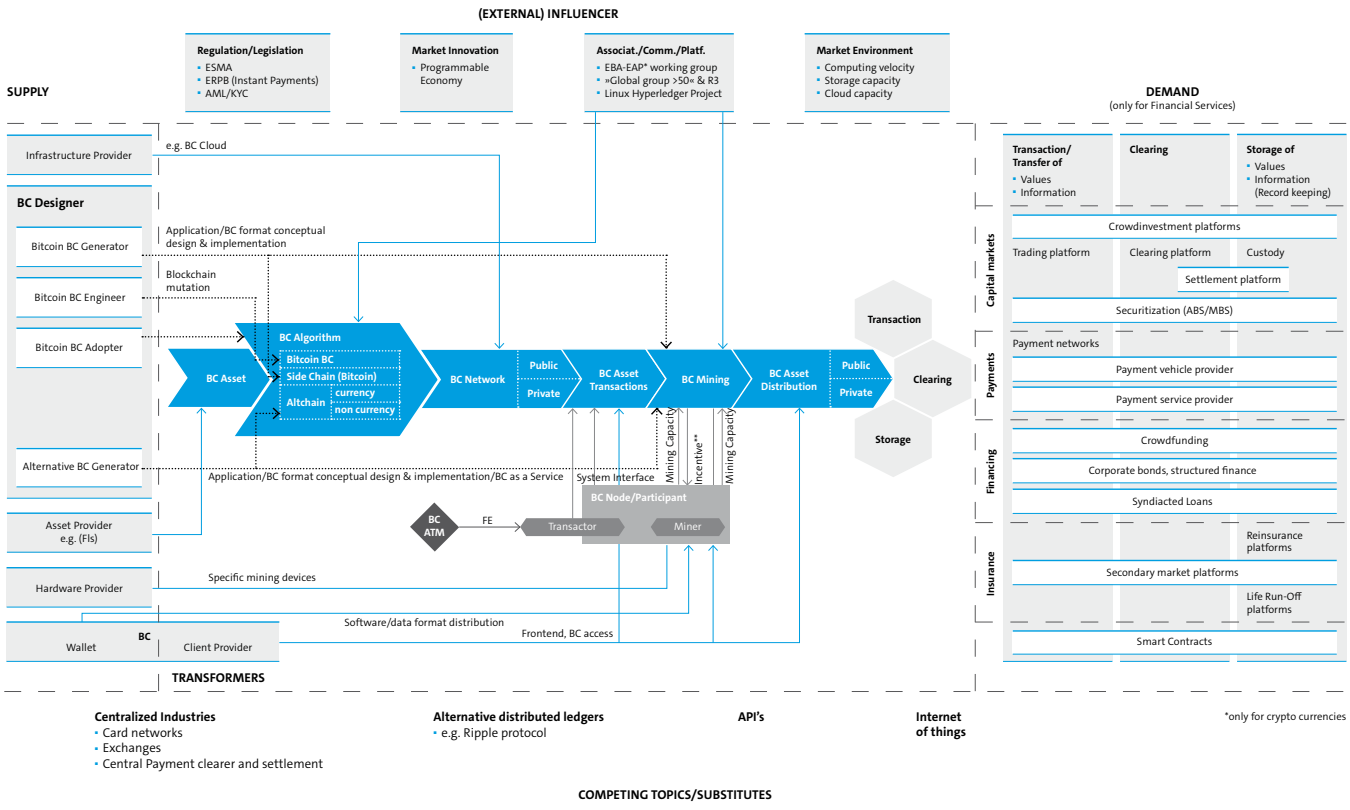


Abbildung 4: Das Ökosystem Blockchain

Eine differenzierte Betrachtung dieser Wertschöpfungskette ermöglicht es, die Kakophonie von Informationen zum und Beteiligten am Thema Distributed Ledger einzuordnen. So zeigen sich eine technisch orientierte Angebotsseite sowie Aufsicht, Regulation und sonstige Interessensgemeinschaften, die aktuell Einfluss bei der Standardisierung auf die Technologie und ihre Anwendung nehmen. Die Nachfrageseite ist von Nutzungsart und Teil-brancheninteressen geprägt. Die zentralen Netzwerkdienstleister – deren Angebote durch DLT substituierbar sind – werden neben determinierenden Technologien die entscheidenden Wettbewerber von Blockchain-Services werden. Der weitere Einsatz von DLT wird zumeist noch in der Form von Proof of Concepts getestet, was in einem etwas unschärferen Bild im Vergleich zum Angebot resultiert.

Die Auseinandersetzung mit den partikularen Einzelinteressen der Stakeholder-Gruppen im Ökosystem Blockchain ist daher angebracht.

3.1 Externe Einflussgrößen

Aufgrund ihrer Bedeutung für die primär betroffenen Teile der Finanzindustrie, also insbesondere für den Wertpapierhandel und den Zahlungsverkehr (näheres dazu siehe auch Folgekapitel), steht die Regulierung durch die European Securities and Markets Authority (ESMA), das EURO Retail Payments Board (ERPB), das European Payments Council (EPC) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) voran.

Die erste Anwendung der Blockchain besteht in der Form des Bitcoins. Dessen zugrundeliegende Philosophie der Unabhängigkeit von einem Finanzinstitut und der darauf folgenden technischen Implementierung erschweren eine Regulierung analog zu Nicht-Kryptowährungen. Überwachung und Regulierung der Geldmenge, Verhinderung von Geldwäsche und Implementierung von Know Your Customer sind weder in der Blockchain, noch in einer der weiteren bisher real existierenden Kryptowährungen realisiert. Mit der zunehmenden Verbreitung der Technologie und der damit einhergehenden Aufmerksamkeit der Regulierungsbehörden sowie systemrelevanter Zulieferer wird das in der Form von neuen Kryptowährungen und Produkten als Altchain zur bestehenden Blockchain oder der Entwicklung von alternativen Distributed Ledgern geschehen. Ein Entwurf hierzu existiert bereits mit dem RSCoin, einer von der Bank of England angeregten, prototypisch entwickelten Kryptowährung. Dieser Entwurf enthält einige der Privacy-Aspekte der ursprünglichen Blockchain, jedoch auch wirksame Mittel zur Regulierung und Steuerung. Der Entwurf versucht mit Anpassungen von Aspekten des Blockchain-Algorithmus Einschränkungen zu umgehen und Eigenschaften wie die Erhöhung der Transaktionsgeschwindigkeit zu verbessern. Ähnliche Entwicklungen sind auch bei Zentralbanken des ESZB, wie dem Vorhaben eines DnB Coin Prototypen der niederländischen Zentralbank, oder der People's Bank of China zu beobachten.

Zusammenschlüsse von Beteiligten am Ökosystem beeinflussen, wie zuvor bereits skizziert, in zunehmendem Maße die Entwicklung und Standardisierung der Technologie und ihre Anwendungsmöglichkeiten. Das Hyperledger Projekt der Linux Foundation ist ein prominentes Beispiel. Das Projekt hat sich zum Ziel gesetzt, die Blockchain Technologie mit Hinsicht auf die Anwend-

barkeit in der globalen Geschäftswelt, branchenübergreifend weiterzuentwickeln. Das Projekt erfreut sich seit seinem offiziellen Start im Februar 2016 regen Zuspruchs aus allen Bereichen der Blockchain-Wertschöpfungskette. Das stattliche Lineup der beitragenden Unternehmen und Organisationen wird in der kommenden Zeit einen signifikanten Beitrag zur Weiterentwicklung der Distributed Ledger-Technologie leisten.

Eine weitere weltweite Initiative fokussiert die Analyse der fünf führenden Blockchain-Varianten unterschiedlicher Anbieter unter Beteiligung einer stetig wachsenden Anzahl an Finanzdienstleistern und Technologieunternehmen unter der Führung der R3. Dabei werden die Banken an ein durch R3, Intel, IBM und Ethereum entwickeltes Blockchain-Netzwerk angeschlossen. Die zugehörige Infrastruktur wird von Microsoft Azure, IBM Cloud und Amazon AWS, drei großen und weit verbreiteten Cloud Providern, bereitgestellt. Ein darauf bereits durchgeführter Pilot-Test einer kleinen Teilgruppe weltweiter Finanzinstitute bestand aus dem Emittieren von Geldmarktpapieren und dem kompletten Handelszyklus. R3 wird diese Initiative vorantreiben und bietet damit eine bankfokussierte Plattform für Blockchain-Initiativen.

Cloud, Crowdfunding, Big Data, Internet of Things und viele weitere Entwicklungsschwerpunkte der letzten Jahre sind inzwischen zur Realität geworden und treiben das Thema, das Gartner »Programmable Economy« nennt, mit großer Geschwindigkeit voran. Die Digitalisierung findet nicht zuletzt Ausdruck in der Programmable Economy, die derzeit branchenübergreifend weiterentwickelt wird. Im Kern schaffen Digitalisierungsprojekte sowohl die fachlichen Anwendungsfälle als auch die technischen Voraussetzungen, um mit digital konsumierbaren Assets Geschäftsprozesse abzuwickeln. Bei vielen Anwendungsfällen in diesem neuen Umfeld muss ein verlässlicher Backbone geschaffen werden, der sowohl die technischen als auch fachlichen Anforderungen an Geschwindigkeit, Verteiltheit, Transaktionssicherheit und Nachvollziehbarkeit abdeckt. Spezialisierte, nicht DLT-basierte Lösungen adressieren einzelne dieser Aspekte, wie z. B. Transaktionsgeschwindigkeit. Hier sind proprietäre Lösungen, wie existierende Zahlungsverkehrssysteme effizienter als ein Distributed Ledger. Diese Technologie kann daher auch nicht als Universallösung für jede verteilte Architektur verwendet werden. Die Summe dieser Fragestellungen beantwortet DLT derzeit jedoch als einzige.

Determinierend für die Weiterentwicklung wird sein, inwieweit das Innovationsgeschehen bei Cloud-, Rechnerleistungs- und Speicherkapazitäten die erforderlichen technischen Rahmenbedingungen bereitstellt, um den größtmöglichen Nutzen aus dem Einsatz der DLT zu realisieren.

3.2 Nachfrager

Die Nachfrageseite im Ökosystem Blockchain differenziert sich nach der Nutzungsart der Technologie. Dabei sind vorrangig drei Anwendungsbereiche zu unterscheiden, die je nach Teilbranche auch in Kombination nachgefragt werden.

Zunächst werden die transaktionsbasierten Nutzer skizziert. Dabei ist zu unterscheiden zwischen Anwendern, die vorwiegend den Informationsaustausch fokussieren, wie z. B. bei

Abstimmverhalten in Jahreshauptversammlungen von Aktiengesellschaften. Auch im Öffentlichen Sektor finden sich dazu Anwendungsfälle, wenn man beispielsweise die klassischen politischen Wahlen in Betracht zieht – wie dies bereits in der Ukraine in der Diskussion war. Andererseits liegt die »natürliche« Anwendung in der Transaktion von Assets; das muss allerdings nicht ausschließlich finanzielle Assets, wie Wertpapiere oder Währungen, betreffen, sondern kann auch Veränderungen von Eigentumsverhältnissen in Katastern oder Grundbüchern umfassen, wie es beispielsweise in Griechenland oder Rumänien bereits angedacht wurde.

Der zweite große Anwendungsbereich – insbesondere im Bankgeschäft – liegt im Bereich Clearing. Dies ist insbesondere im Zahlungsverkehr und Wertpapiergeschäft von Bedeutung, wo die größten Effizienzgewinne und das umfassendste Veränderungspotential zu erwarten sind. Darauf wollen wir ausführlich in folgenden Kapiteln eingehen.

Der Bereich der Asset- und Informationsspeicherung und Weitergabe ist aus Anwendersicht von höchster Bedeutung beim Einsatz dezentraler Technologien. Dabei ist wie bereits im erstgenannten Anwendungsbereich zwischen der Speicherung und Distribution von Assets und von Informationen zu differenzieren.

Bei der Speicherung und Distribution von Assets ist insbesondere an jede Form von Transaktionsregistern zu denken, die für die Risikobewertung neuer Handelsaktivitäten von wesentlicher Bedeutung sind. Dasselbe gilt für das Settlement von Handelsgeschäften und die damit verbundenen Aufgaben in der Wertpapierverwahrung. Die Vielzahl der Anwendungsbereiche bei corporate actions scheint endlos.

Darüber hinaus ist die dezentrale Verfügbarkeit von sogenannten finanziellen Informationsdaten bei der Bonitäts- bzw. Rating-Einstufung bei Finanzgeschäften sowohl im Provisions- als auch im Zinsgeschäft zur Hebung von Effizienzvorteilen von hoher Bedeutung. Dies gilt sowohl im Primärmarkt bei der Emission von Wertpapieren, der Ausgabe von Kreditfaszilitäten als auch der Übernahme von Versicherungsrisiken; aber auch im Sekundärmarkt bei ABS oder MBS-Transaktionen, im Wertpapierhandel oder in der Rückversicherung bzw. dem Run-off-Geschäft sind die Vorteile der dezentralen Verfügbarkeit von Primärmarktinformationen im Rahmen von DLT-Lösungen mit hohen Effizienzpotentialen verbunden.

Eine Vielzahl Anwendungsmöglichkeiten eröffnet sich für das Teilen und Bearbeiten von hoheitlichen Informationen zwischen nationalen und supranationalen Organisationen, wie das ESZB, die nationalen wie europäischen Aufsichtsbehörden EBA, ESMA und EIOPA mit fiskalischen Behörden. Inwiefern zukünftig große zentralistische Reportinganforderungen im Rahmen eines European Reporting Framework, wie sie heute noch vorgesehen sind, zu sehen sein werden, ist zumindest fraglich. Hier würden Änderungen zu einer erheblichen Entlastung der meldepflichtigen Marktteilnehmer führen.

Schließlich ist noch auf eine bedeutende Anwenderklientel hinzuweisen, die insbesondere über sogenannte Smart Contracts von der Technologie profitiert. Neben der hier nicht näher diskutierten Versicherungsindustrie, deren Anwendungsgebiete in Bezug auf kausalbezogene sowie zeitlich begrenzte Versicherungsleistungen auf der Hand liegen (z. B. Transportversicherungen in der Verbindung des Internet of Things), sind beispielsweise im Trade Finance-Geschäft interessante Zug-um-Zug Geschäfte zwischen den Beteiligten zumeist internationalen Akteuren sehr vereinfacht denkbar. Komplexe Projektfinanzierungen, syndizierte Kredite, Dokumentenakkreditive, Rembourskredite oder sonstige Exportfinanzierungen sind damit unter ganz neuen Effizienzgesichtspunkten zu betrachten. Der bereits seit längerem anhaltende Trend des Ausdünnens von Korrespondenzbanken-Netzwerken würde sich mit dem Einsatz von DLT-Smart Contracts beschleunigen.

Mit welcher Geschwindigkeit diese Veränderungen Einzug halten werden, ist wesentlich von den spezifischen DLT-Angeboten und der Spezialisierung ihrer Zulieferer abhängig.

3.3 Zulieferer

Die Seite der Zulieferer lässt sich anhand der Wertschöpfungskette der Blockchain strukturieren. Die zentrale Komponente, digital konsumierbare Assets wie z. B. Wertpapiere, Währungen, Versicherungsverträge, Grundbucheinträge etc. wird von Asset Providern gestellt. Das Asset prägt das gewählte Protokoll, die gewählte Technologie und den Zugang zum Distributed Ledger Netzwerk. Es bestimmt, welche gesetzlichen Vorschriften berücksichtigt und gegebenenfalls im Protokoll implementiert werden müssen. In der Finanzindustrie übernehmen diese Rolle im Wesentlichen Banken. Als Asset kann alles dienen, was in digitaler Form konsumier- oder handelbar ist.

Blockchain-Designer entwerfen basierend auf existierenden oder neu entwickelten Protokollen neue Anwendungen mit Hilfe der Distributed Ledger Technologie. Bitcoin oder weitere alternative Kryptowährungen wie Ethereum, Dogecoin oder Litecoin sind dabei beispielhaft zu nennen. Darüber hinaus wird eine große Zahl weiterer Anwendungen und Frameworks, z. B. für Smart Contracts oder abstrakte Assets entwickelt und angeboten. Diese sind – wie die zugrundeliegende Technologie – meist unter Open Source Lizenzen erhältlich. Treiber dieser Innovationen sind derzeit noch größtenteils Start-ups aus der Finanz- oder Technologiebranche.

Infrastrukturprovider stellen öffentliche oder private Netzwerke als Basis für die DLT zur Verfügung. Je nach Anwendungsfall können dafür bereits existierende Verbindungen genutzt werden. Auf Basis des physischen Netzwerkes bestimmen die Eigentümer den Zugang zu Funktionen des Blockchain-Netzwerks. Hierbei sind Mischformen möglich; so kann z. B. ein ausschließlich privater Zugang zum Handel auf einer Plattform existieren, das Mining jedoch öffentlich zugänglich und incentiviert sein.

Cloud Infrastrukturprovider bieten im Rahmen ihres existierenden Angebots elastische Rechnerkapazitäten an, auf denen Komponenten einer DLT-basierten Anwendung laufen. Zu diesen klassischen Angeboten, die ausschließlich reine Rechenleistung anbieten, haben einige Dienstleister Blockchain-as-a-Service-Lösungen entwickelt, die sowohl Prototyping, als auch ausgereifte Lösungen für den Massenmarkt unterstützen können.

Das Mining, das z. B. die Blockchain benötigt, stellt sehr hohe Anforderungen hinsichtlich Rechenkapazität an die Teilnehmer des Netzwerkes. Einige Hardwarehersteller haben darauf reagiert und bieten für Mining spezialisierte Computer an. Diese sind gerade im Umfeld von Kryptowährungen sehr häufig anzutreffen, da diese Netzwerke öffentlich sind und die Geldschöpfung meist ausschließlich durch Mining geschieht.

Für den Zugang zu Distributed Ledger-basierten Anwendungen und damit zu Asset-Transaktionen, werden Clients, wie z. B. Wallets für Kryptowährungen, benötigt. Für den Bitcoin existieren z. B. neben den vom Bitcoin Core zur Verfügung gestellten Lösungen viele Alternativen. Die meisten werden, wie auch Bitcoin selbst, unter einer Open Source Lizenz wie der MIT License des Massachusetts Institute of Technology oder der GNU General Public License (GPL) angeboten.

Neben Wallets gibt es für alle Architekturebenen und Anwendungen entsprechende Software wie z. B. Trading Applikationen, Software-basierte Miner, APIs für die Anbindung von Shopsystemen etc. Bitcoin, als erste Anwendung der Blockchain, ist auch deshalb so erfolgreich, weil das IT-Ökosystem inzwischen für fast jeden Zugang und jeden Anwendungsfall Lösungen bereithält, auf denen Mehrwertdienste entstehen können.

3.4 Prozessoren

Prozessoren zeichnen sich durch einen operativen Beitrag zu einer DLT-basierten Lösung aus. Die Prozessoren lassen sich in drei große Kategorien einteilen: Provider technischer Lösungsbestandteile, Betreiber privater Distributed Ledger Netzwerke und Betreiber von Peripheriefunktionen.

Eine Cloud-basierte Wallet-Lösung zur »Aufbewahrung« der digitalen Assets oder ein Cloud-basierter Trading Client sind zwei Beispiele für technische Lösungsbestandteile, die nicht nur einmal zum Installationszeitpunkt oder während der Entwicklung der Lösung eingekauft und verwendet werden. Diese Bestandteile werden im klassischen Cloud-Modell gehostet und betrieben. Sie können feste Bestandteile einer DLT-basierten Anwendung sein, oder komplementär zu einem existierenden, öffentlich zugänglichen Netzwerk gestaltet sein. Produktiv eingesetzte Beispiele hierfür sind Wallet-Lösungen für Bitcoin wie Coinbase, Blockchain.info oder BitGo.

Private Netzwerke sind derzeit noch größtenteils in der Erprobung und in der Form von Proof of Concepts vorhanden. Es gibt jedoch zurzeit in der Finanzdienstleistungsindustrie einen starken Trend zur Weiterentwicklung, damit privaten Netzwerken ggfs. auch unter der Verwendung einer alternativen DLT effektiv einige Schwächen aus regulatorischer Sicht beseitigt und technische Einschränkungen entfernt werden können. Private Netzwerke können die Anonymität der

Marktteilnehmer aufheben, sowie das Mining abschaffen. Das Mining dient als Alternative zu einer expliziten Trust-Beziehung zwischen den Netzwerkteilnehmern, indem es den Proof of Work Mechanismus nutzt, um Betrugsversuche unrentabel teuer zu machen. In einem Netzwerk mit Trust-Beziehungen zwischen den Teilnehmern und der damit einhergehenden Transparenz ist dieser Aspekt nicht mehr notwendig.

Die dritte Gruppe, die Betreiber von Peripheriefunktionen, stellt Plattformen und Dienste bereit, um die Interaktion mit der realen Welt zu ermöglichen. Exchange- und Handelsplattformen wie z. B. Kraken oder Linq bieten die Möglichkeit, echte in virtuelle Assets zu verwandeln und umgekehrt oder die virtuellen Assets zu handeln. Wie der Fall Mt. Gox gezeigt hat, ist diese Gruppe mit Risiken konfrontiert. Eine Folge hiervon ist der stetige und schnelle Wandel – Unternehmen entstehen und verschwinden in hohem Tempo.

3.5 Korrelierte Themengebiete

Der Wunsch, die Anonymität der Netzwerkteilnehmer aufzuheben oder zumindest zu begrenzen, Alternativen zum Mining zu finden oder auch nur den Zugang bestimmen zu können, hat zur Entwicklung zahlreicher Modelle für private Blockchains, aber auch zu Alternativen zur Blockchain Technologie nach Satoshi Nakamoto geführt. Prominentestes Beispiel ist das auf Payments ausgerichtete Ripple-Protokoll. Das Ripple-Protokoll stellt im Kern, dem Ripple-Network, einen Distributed Ledger zur Verfügung, der einen Konsens-Mechanismus nutzt, der kein Mining wie in der Blockchain benötigt. Die Netzwerkteilnehmer sind bekannt und so kann Ripple auf diesen zusätzlichen Schutzmechanismus verzichten. Neben dem Ripple-Network bietet Ripple mit Ripple Connect und Ripple Stream Zugänge für Banken und Market Maker an. Eine weitere DLT ist Corda von R3. Hier wurden, wie bei Ripple, Design-Entscheidungen getroffen, die den Anforderungen von Finanzinstituten in den kritischen Aspekten besser gerecht werden sollen, als die Blockchain es tut.

Der Einbau von Nodes, die dem Regulator, der Aufsicht bzw. dem Controlling dienen und das Vermeiden von Mining – und damit einhergehend mehreren möglichen Konsens-Algorithmen – sind die ersten logischen Anpassungen. Eine weitere grundlegende Abweichung ist der Fokus auf die von Corda als »Agreements« bezeichneten Smart Contracts. Diese werden mit natürlich-sprachlichen juristisch relevanten Dokumentinhalten verlinkt, sodass man nicht nur über Transaktionen kommuniziert, sondern sofort auch Verträge und deren juristisches Beiwerk tauscht. Einschränkungen des Protokolls im Vergleich mit der restlichen Familie der Distributed Ledger Lösungen finden sich mit Bezug zum Verteilen der Daten und der Konsensfindung. So werden die Daten innerhalb eines Agreements nicht allen Teilnehmern zur Verfügung gestellt und der Konsens wird auch nur zwischen den an einem Agreement beteiligten Parteien gefunden. Das Designziel ist hierbei eine leichtere Integrierbarkeit in bestehende Systeme und Abläufe. Noch ist Corda neu und muss seine behaupteten Vorteile unter Beweis stellen.

Komplementäre Entwicklungen wie APIs aus den Digitalisierungsinitiativen und das Internet of Things (IoT) wirken als Katalysator für die Nutzung und Weiterentwicklung der DLT und darauf aufbauender Anwendungen und deren Services.

Neben den technologisch getriebenen Themen sind es vor allem die bereits existierenden Handelsplätze und Börsen, die bereits Marktzugänge und Funktionen für die Teilnahme am Handel bieten. Zusammen mit zentralisierten Industrien wie das Payment Netzwerk SWIFT oder Card Provider stellen sie Dienste zur Verfügung, mit denen die DLT und ihre Anwendungen konkurrieren. Die Auswirkungen der Nutzung von DLT in diesen Bereichen und mögliche Modelle werden im Folgenden aufgeführt und diskutiert.

4 Anwendung des Distributed Ledger

4 Anwendung des Distributed Ledger

4.1 Bitcoin – Der Ursprungs-Blockchain Use Case

Der Bitcoin hat sowohl technologisch als auch fachlich konzeptionell den Grundstock für Kryptowährungen gelegt. Er hat grundlegende Probleme der bis dato in der Theorie existierenden Währungen gelöst und ist nach seinem Start im Januar 2009 inzwischen die Kryptowährung mit der höchsten Marktkapitalisierung. Oft totgesagt behält er dennoch seine Relevanz. Im Laufe der Zeit haben sich Trittbrettfahrer, wie z. B. Omni (ehemals Mastercoin) hinzugesellt, die die Infrastruktur des Bitcoins nutzen und ihre eigene Kryptowährung mit ihrer Hilfe realisieren. Diese bieten in der Regel zusätzliche Funktionalität, indem sie das Protokoll erweitern und damit z. B. den Handel von Wertpapieren oder ähnlichem ermöglichen. Diese Art der Erweiterung wird auch als »Colored Bitcoin« oder »Colored Coin« bezeichnet.

Neben dem in Kapitel 3 beschriebenen Ökosystem sind bei Bitcoin vor allem die Miner hervorzuheben. Das größte Blockchain Netzwerk des Planeten verbraucht in etwa halb so viel Energie wie Irland. Die Anzahl der Miner, die den Großteil dieses Energieverbrauches repräsentieren, ist nicht genau bekannt. Der größte Teil der Blöcke wird von Mining-Pools verarbeitet, über die selten bekannt ist, wie viele Nodes und Eigentümer letztendlich dahinterstehen. Die Mining-Pools sind derzeit überwiegend in China zu finden. Dort hat die Kryptowährung nach einem ersten Verbot wieder an Beliebtheit gewonnen, bietet sie doch Anonymität.

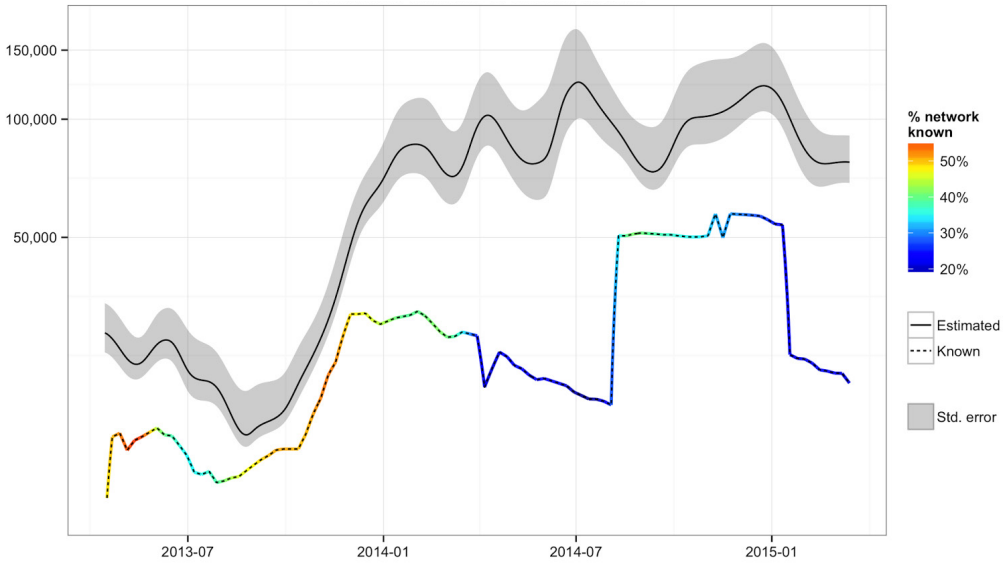


Abbildung 5: Geschätzte Anzahl von Bitcoin-Minern im Zeitraum Mitte 2013 bis Anfang 2015.[24]

24 Organofcorti.blogspot.de.
↗ http://organofcorti.blogspot.de/2015/03/march-15th-2015-network-statistics.html

Aktuelle Kennzahlen des Netzwerkes werden z. B. von Blockchain Luxembourg S.A. (www.blockchain.info) veröffentlicht und spiegeln das lange Bestehen der Kryptowährung. Die Blockbildung hat sich in den letzten drei Jahren bei durchschnittlich zehn Minuten eingependelt, pro Block sind es ca. 1500 Transaktionen. Die Blockchain wächst beständig und ist im Jahr 2016 bei ca. 85 GB und 160 Millionen Transaktionen angekommen. Eine Transaktion ist ca. 550 Bytes[25] groß, was bei der derzeit zur Verfügung stehenden Technologie eine breitflächige Anwendung – z. B. im Zahlungsverkehr – unmöglich macht.

Bei allen Teilnehmern am Ökosystem, seien es Wallet-Anbieter, Exchanges oder Miner steht die Frage der Finanzierung im Raum. Miner erhalten für ihre Tätigkeit Bitcoins, was neben der Incentivierungsfunktion auch zur Sicherheit des Netzwerkes beiträgt. Transaktionen sind grundsätzlich kostenlos. Einige Miner ermöglichen es jedoch, gegen Gebühr, Transaktionen bevorzugt zu bearbeiten und damit die Ausführungszeit niedrig zu halten. Die Summe dieser Gebühren schwankt und liegt Stand Oktober 2016 bei 68 BTC.

Der Bitcoin ist schon aufgrund seiner Stellung als Urvater der aktuellen Kryptowährungen und seiner Marktkapitalisierung ein Barometer und Orakel für die weitere Entwicklung. Kryptowährungen werden sich weiterentwickeln, aber die Relevanz des im Vergleich zu den Smart Contracts auf Ethereum oder Eris konzeptionell einfachen Bitcoins ist und bleibt allen anderslautenden Stimmen zum Trotz bisher ungebrochen.

4.2 Das Ripple-Protocol als Alternative zur Blockchain

Ripple muss aus mehreren Blickwinkeln betrachtet werden. Zuerst genannt sei die technische Implementierung. Ripple verwendet technische Komponenten der Blockchain, weicht in entscheidenden Punkten aber von deren Architektur ab. Der von Ripple genutzte Konsensmechanismus Ripple Protocol Consensus Mechanism ist für eine Nutzung in einem privaten oder konsortialen Netzwerk konzipiert. Jeder Node im Netzwerk bestimmt eine Liste von Validator Nodes, die seine Transaktionen validieren. Hier muss also Vertrauen außerhalb des Netzwerks hergestellt werden. Ebenso gibt es Nodes, die als Market Maker oder als Zugang für den Regulator dienen.

25 Quelle: ↗ https://tradeblock.com/bitcoin/historical/1h-f-tsize_per_avg-01101

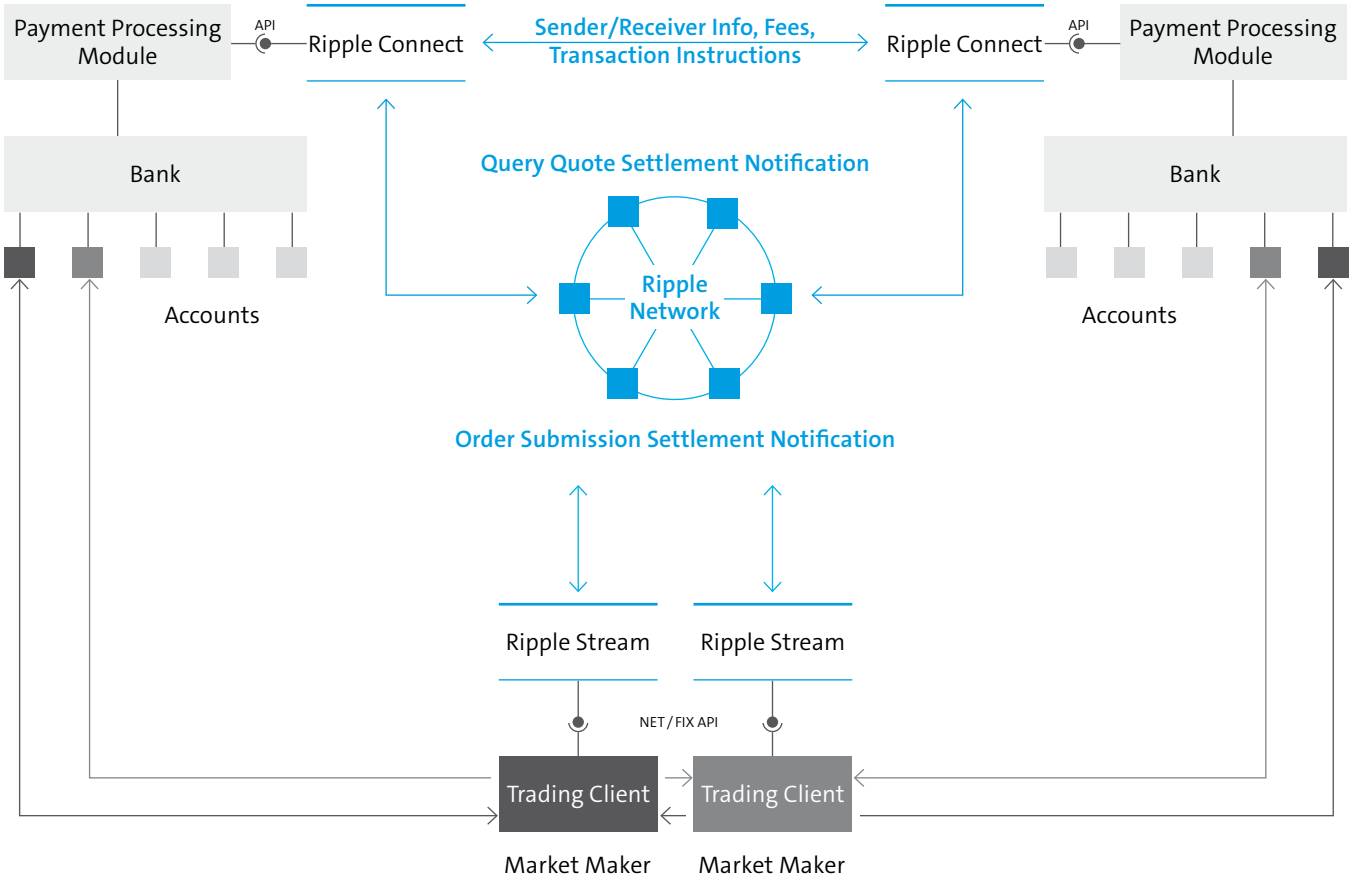


Abbildung 6: Ripple Netzwerk[26]

Das Protokoll und die Architektur sind für Zahlungstransaktionen konzipiert und damit widmen wir uns dem zweiten Blickwinkel. Ripple als Unternehmen bietet einen, den der bisherigen Zahlungsverkehrsnetzwerkanbieter wie z. B. SWIFT gleichenden, Service an. Teilnehmer am Netzwerk können mithilfe des Ripple Protokolls und des Ripple Netzwerks Zahlungen schnell abwickeln – die entsprechende Integrierbarkeit in deren Systemlandschaft und Prozesse vorausgesetzt.

Hier ist Folgendes von Bedeutung: Wer Ripple nutzt, nutzt den Service eines Unternehmens, aber nicht die Blockchain an sich. Dabei sind neben der, im Vergleich zu existierenden Providern, noch nicht konkurrenzfähigen Anzahl an Netzwerkteilnehmern, auch die bekanntermaßen aus der Zusammenarbeit mit Unternehmen des Alters und der Größe von Ripple erwachsenden Risiken zu beachten.

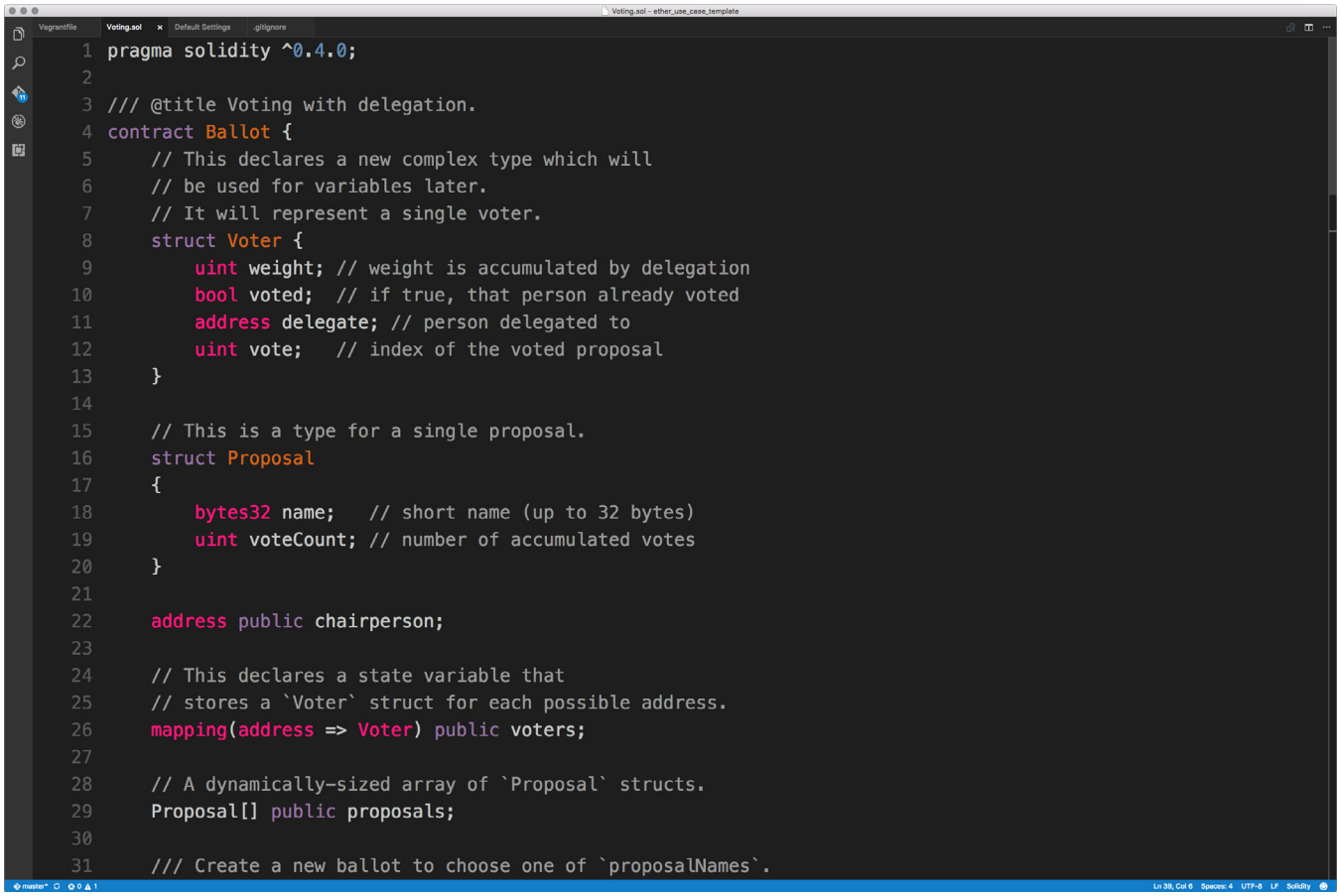
26 Quelle: ↗ Ripple.com

4.3 Technische Abbildung von Smart Contracts

Unter Smart Contracts (auch »intelligente« bzw. »verdinglichte« Verträge) versteht man Programme bzw. Transaktionsprotokolle, die automatisch und in Echtzeit die Einhaltung vertraglich vereinbarter Bestimmungen überwachen und automatisiert die hieran geknüpften Rechtsfolgen durchsetzen, sofern die zugrunde gelegte Bedingung eintritt.[27] Im weiteren Verlauf wird die technische Abbildung von Smart Contracts am Beispiel der Ethereum-Blockchain ausgeführt.

Die Ethereum-Blockchain versteht sich als »World Computer«. Dies wird deutlich, wenn man sich der technischen Funktionsweise der Smart Contracts auf Ethereum widmet. Entwickelt werden Smart Contracts in der eigens dafür entwickelten Sprache Solidity. Solidity ist eine abstrakte Programmiersprache, die in Struktur und Syntax JavaScript ähnelt und deren Compiler die Contracts in Code für Ethereum umwandelt.

27 So schon 1994 beschrieben von Nick Szabo: Smart Contracts.
↗ http://szabo.best.vwh.net/smart.contracts.html



```
pragma solidity ^0.4.0;

/// @title Voting with delegation.
contract Ballot {
    // This declares a new complex type which will
    // be used for variables later.
    // It will represent a single voter.
    struct Voter {
        uint weight; // weight is accumulated by delegation
        bool voted;  // if true, that person already voted
        address delegate; // person delegated to
        uint vote;   // index of the voted proposal
    }

    // This is a type for a single proposal.
    struct Proposal
    {
        bytes32 name;   // short name (up to 32 bytes)
        uint voteCount; // number of accumulated votes
    }

    address public chairperson;

    // This declares a state variable that
    // stores a `Voter` struct for each possible address.
    mapping(address => Voter) public voters;

    // A dynamically-sized array of `Proposal` structs.
    Proposal[] public proposals;

    /// Create a new ballot to choose one of `proposalNames`.
```

Abbildung 7: Beispiel Code für einen Smart Contract in der Sprache Solidity

Quelle: Screenshot NTT Data – Ausschnitt aus frei verfügbaren Tutorial von
↗ http://solidity.readthedocs.io/en/develop/solidity-by-example.html

Kompilierte Smart Contracts sind JavaScript Dateien, die mittels des web3-APIs mit der Ethereum-Blockchain interagieren. Sie reagieren auf Veränderungen des Ledgers und können ihrerseits den Ledger verändern. So können sich Contracts untereinander an ihre Accounts oder an Nicht-Contract Accounts Ether übertragen. Die Interaktion zwischen Contracts über deren Funktionen ist ebenfalls möglich. Obwohl Solidity als Sprache im Vergleich zu sonst üblichen Programmiersprachen schlicht erscheint, ist es möglich sehr komplexe Konstrukte zu entwickeln; so stecken hinter den Elementen die Mächtigkeit und Komplexität der Ethereum-Blockchain-Implementierung. Wer den Zugang zu einem Node hat, kann mit den Smart Contracts ebenfalls über das web3-API interagieren.

Wenn der Contract in JavaScript kompiliert wurde, dann kann er über einen lokalen Node (Node im Zugriff des Smart Contract Entwicklers) auf die Ethereum Blockchain übertragen werden. Die JavaScript Programme werden dann analog zu Transaktionen in einem Mining-Prozess aktiviert und auf alle Nodes des Netzwerkes verteilt. Ab diesem Zeitpunkt werden sie von allen Nodes im

Netzwerk ausgeführt. Das gesamte Netzwerk agiert hiermit als virtueller Computer für die Ausführung von Smart Contracts.

Solidity unterstützt gängige Konzepte der Softwareentwicklung, so werden z. B. automatisierte Tests unterstützt. Tools wie z. B. Truffle, ein Entwicklungsframework für Solidity, stellen Testframeworks zur Verfügung, um diese analog zu gängigen Continuous Integration Tools in den Softwareentwicklungsprozess zu integrieren. Die Komplexität der zugrundeliegenden Blockchain und die Interaktion zwischen Smart Contracts in einer hinreichend komplexen Lösung stellen auch erfahrene Entwickler vor große Herausforderungen. Dies wurde bei der Krise der The DAO, die erste dezentrale, autonome Organisation (Decentralized Autonomous Organization, DAO) auf der Ethereum Blockchain, ersichtlich. Diese Organisation besteht ausschließlich in der Form von Smart Contracts und bildet effektiv eine Crowdfunding-Kampagne ab. Mitglieder der The DAO können über die Smart Contracts Wahlen zur Verwendung der gesammelten Gelder (in der Form der Ethereum Kryptowährung Ether) abhalten. Ein Angreifer hat eine Lücke in der Implementierung der Smart Contracts der The DAO ausgenutzt, um Gelder aus der The DAO abzuziehen. Ethereum reagierte hierauf mit einem sogenannten »Hard Fork«, einer Änderung an der Implementierung des Protokolls, die das Ausgeben der abgezogenen Gelder unmöglich machen sollte. Dies führte letztendlich zur Aufspaltung der Chain in Ethereum und Ethereum Classic, da nicht alle Miner von Ethereum ausschließlich die neue Version von Ethereum bedienen. Eine weitere Folge war eine erneute und sehr detailliert geführte Auseinandersetzung, wie die technische Perspektive von Smart Contracts und die rechtliche Perspektive korrelieren.

4.4 Use Cases in Wirtschaft und Gesellschaft

Wie geschildert, bildet die Basis aller Entwicklungen die Kryptowährung Bitcoin. Darüber hinaus haben sich inzwischen jedoch auch viele weitere Bereiche mit der zugrundeliegenden Blockchain beschäftigt. Das große Interesse an Blockchain hat seinen Ursprung in den vorhergesagten Auswirkungen auf bestehende Technologien und Geschäftsmodelle, aber auch in den gesamtgesellschaftlichen Folgen.

Die drei größten potentiellen Verschiebungen sind hier noch einmal zusammengefasst:

- Übernahme oder Transformation der Aufgaben des Mittelsmanns[28] (z. B. in Gestalt des Notarwesens für Rechtsgeschäfte oder Abrechnungsstellen im Finanzwesen,[28] denen eine der wichtigsten Rollen im derzeitigen Wirtschaftssystem zukommt). Smart Contracts und Smart Property sind hier zwei Beispiele für angestoßene Entwicklungen.
- Einführung von Knappheit und Einmaligkeit von digitalen Entitäten, in Analogie zu den aus der physischen Welt bekannten Eigenschaften von Dingen;[29] langfristige Transformation des klassischen Webs zum Value Web.[30] Die Kryptowährung übernimmt die Rolle von Gold im digitalen Raum.
- Weiterentwicklung der zentralisierten digitalen Netzstrukturen zu einer offenen und skalierbaren digitalen Ökonomie[31].

Speziell im Finanz- und Geldwesen werden bereits konkretere Technologieanwendungen thematisiert:

- Erschaffung neuartiger Zahlungsstrukturen (z. B. Micropayments), die aufgrund der Gebührenstruktur heutiger Systeme nicht denkbar sind.[32]
- Entwicklung von Notenbank-unabhängigen Währungssystemen.[33]
- Etablierung von Finanztransaktionen außerhalb des klassischen Bankensystems (Auflösung bekannter Prozesse, wie etwa gebührenpflichtiger Auslandsüberweisungen[34]).

Außerdem ergeben sich neuartige Anwendungen für Datenverarbeitungssysteme:

- Entwicklung von immanent nicht-manipulierbaren Datenbanktypen.[35]
- Etablierung eines Standards für »Timestamping«[36] in verteilten Systemen.[37]

28 Aaron Wright, Primavera De Filippi, »Decentralized Blockchain technology and the rise of Lex Cryptographia«.
↗ https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

29 Christoph Bergmann, bitcoinblog.de
↗ http://bitcoinblog.de/2014/11/17/es-ist-die-blockchain-nicht-der-bitcoin-wirklich

30 Chris Skinner, thefinanser.com
↗ http://thefinanser.com/2015/02/forget-fintech-welcome-to-the-valueweb.html

31 Michael Crosby (Google) et al., »BlockChain Technology Beyond Bitcoin«.
↗ http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

32 Sajith Pai, INMA. ↗ http://www.inma.org/blogs/tech-trends/post.cfm/beyond-bitcoin-to-the-blockchain-what-it-means-for-news-publishers

33 Vruti Desai, Surtadja Center. ↗ http://scet.berkeley.edu/blockchain-kick-off-event-at-scet

34 Randy Komisar, Kleiner, Perkins, Caufield and Byers.
↗ http://www.kpcb.com/blog/the-real-reason-why-blockchain-technology-is-worth-investing-in

35 Christoph Bergmann, bitcoinblog.de
↗ http://bitcoinblog.de/2014/11/17/es-ist-die-blockchain-nicht-der-bitcoin-wirklich

36 Diverse Autoren. https://en.wikipedia.org/wiki/Block_chain_(database) und
↗ https://en.wikipedia.org/wiki/Trusted_timestamping

37 Nick Grossman, Union Square Ventures. ↗ http://www.nickgrossman.is/2015/06/15/the-blockchain-as-time

Abbildung 8[38] präsentiert eine Auswahl an Marktpotenzialen für die Blockchain-Technologie. Wie bereits besprochen ist eines der elementaren Projekte für die Weiterentwicklung der Blockchain-Technologie in Richtung Smart Contracts die Ethereum-Blockchain.[39]

Das Mastermind hinter Ethereum, Vitalik Buterin, war einer der ersten, die verstanden hatten, dass Zahlungen ohne Mittelsmänner möglich sind und er war derjenige, der das Vorstellungsvermögen besaß, dass dieser Mechanismus prinzipiell auf alle Arten von Verträgen übertragbar ist.[40] Er und sein Team entwickeln mit Ethereum eine programmierbare Blockchain, die selbstausführende, digitale Vertragswerke zur Normalität werden lässt.[41] Das Start-up Everledger setzt mit seiner Plattform zur Betrugsaufdeckung im Diamantenhandel bereits erfolgreich auf eine Smart Contract Implementierung einer privaten Blockchain.[42]

Der Vorreiter unter den Börsenanwendungen ist ein, von der größten elektronischen Börse der USA Nasdaq, entwickeltes Produkt, das die Anteile von pre-IPO Unternehmen für den Handel aufbereitet. Das Linq genannte Produkt setzt dabei, anders als die Entwicklungen der Großbanken, auf die offene Blockchain des Bitcoin-Netzwerks und ist seit Herbst 2015 im Einsatz.[43] Ein Beispiel für Micro- oder Nanopayments ist das Projekt SatoshiPay.[44]

38 Saad Hirani, Sutardja Center. ↗ http://scet.berkeley.edu/beyond-bitcoin-in-the-world-of-blockchain

39 White-Paper Ethereum. ↗ https://github.com/ethereum/wiki/wiki/White-Paper

40 Frank Schmiechen, Gründerszene. ↗ http://www.gruenderszene.de/allgemein/blockchain-wie-geht-das

41 Hannes Grassegger, Capital.de Reportage. ↗ http://www.capital.de/dasmagazin/der-digitale-lenin-hinter-der-blockchain.html

42 Luke Parker, Brave NewCoin. ↗ http://bravenewcoin.com/news/everledger-uses-the-blockchain-tackling-conflict-diamonds-and-insurance-fraud

43 Sarah Todd, American Banker. ↗ http://www.americanbanker.com/news/bank-technology/nasdaq-signals-confidence-in-bitcoin-not-just-the-blockchain-1074405-1.html

44 SatoshiPay Webseite. ↗ https://satoshipay.io

Abbildung 8: Beispielhafte Blockchain-Technologie Anwendungen[45]

Erste Vorstöße im Bereich Smart Property macht Honduras[46] und der US-amerikanische Bundesstaat Vermont überdenkt den Einsatz einer Blockchain basierten Regierungsstatistik.[47] Im Bereich Datenbanklösungen bietet das Berliner Start-up Ascribe eine erste Lösung auf Blockchain-Basis an.[48] Das Unternehmen Verisart bereitet den Weg für den Einsatz von Blockchain für Produkte zum Sichern des geistigen Eigentums – ihre derzeitige Lösung prüft und sichert Preise von Kunstobjekten ab.[49] Als Konkurrent von Uber versteht sich das Start-up Arcade City und bietet eine dezentrale Lösung für Ride-Sharing an, die dank Blockchain-Ansatz höhere Margen für Fahrer verspricht.[50]

Im schnell wachsenden Markt des Internet of Things (IoTs) gilt die Blockchain als potentieller Problemlöser drei noch nicht bezwungener Herausforderungen: der minimalen Wertschöpfung pro Gerät, der Sicherheit des Gesamtnetzes und der Kostendeckung für Konnektivität.[51] Die drei grundsätzlichen Eigenschaften einer IoT-tragfähigen dezentralen Architektur (siehe Abbildung 9 – Blockchain als digitales Konto – Transaktionen zwischen Geräten im IoT) für Transaktionen werden in hohem Maße durch die Blockchain-Technologie als Transaktionsprotokoll abgedeckt:

45 Saad Hirani, Sutardja Center. ↗ http://scet.berkeley.edu/beyond-bitcoin-in-the-world-of-blockchain

46 Peter Kirby, Open Letter Factom.
↗ https://www.factom.com/a-humble-update-on-the-honduras-title-project

47 Brian Forde, Michael Casey. wired.co.uk
↗ http://www.wired.co.uk/news/archive/2016-01/05/blockchain-is-the-new-signature

48 Kim Rixecker, t3n. ↗ http://t3n.de/news/bigchaindb-blockchain-datenbank-679337

49 Florian Graillot. Techcrunch.
↗ http://techcrunch.com/2015/10/03/the-blockchain-might-be-the-next-disruptive-technology

50 Joel Valenzuela, cointelegraph.
↗ http://cointelegraph.com/news/arcade-city-decentralized-blockchain-based-answer-to-uber

51 Ryan Begley, IBM Big Data and Analytics Hub.
↗ http://www.ibmbigdatahub.com/blog/what-blockchain-and-what-does-it-have-do-internet-things

vertrauensfreie Peer-to-Peer-Kommunikation, sicherer verteilter Datenaustausch und eine skalierbare Art der Gerätekoordination.

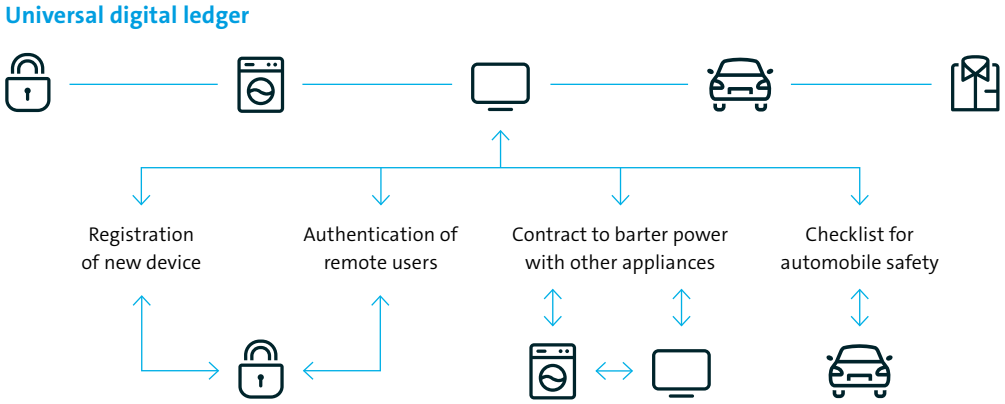


Abbildung 9: Blockchain als digitales Konto – Transaktionen zwischen Geräten im IoT[52]

Samsung und IBM arbeiten zusammen an einem Build of Proof-Konzept für das IoT, welches im Aufbau IBMs ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) Konzept folgt.[53]

Auch der deutsche Mischkonzern Bosch betreibt in seinem »Internet of Things & Services Lab« Forschung zur Blockchain.[54] Sensing-as-a-Service ist ein dort entwickelter Vorschlag für ein Geschäftsmodell der Blockchain im IoT.[55] Das Start-up slock.it und der Industriekonzern RWE arbeiten an einer Blockchain-Lösung für Zahlvorgänge im Elektromobilitätszeitalter: unmittelbare und autonome Abwicklung der Zahlungstransaktion zwischen Fahrzeug und Ladestation, ohne Eingriff des Fahrzeugführers.[56]

52 Veena und Brody, IBM Executive Report, «Device democracy: Saving the future of the Internet of Things”.
↗ http://www.ibmbigdatahub.com/blog/what-blockchain-and-what-does-it-have-do-internet-things

53 Colin Barker, zdnet.com. ↗ http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be

54 Markus Weinberger, Bosch Connected World Blog.
↗ http://blog.bosch-si.com/categories/business-models/2015/06/bitcoin-enabler-for-the-iot

55 Kay Noyen et al., »When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin”.
↗ http://cocoa.ethz.ch/downloads/2014/09/1749_main.pdf

56 Christoph Bergmann, BitcoinBlog.de
↗ http://bitcoinblog.de/2016/02/26/rwe-und-slock-it-wollen-ethereum-fuer-elektroautos-nutzen

5 Rechtliche Überlegungen zu Blockchain und einzelnen Anwendungen, insbesondere Kryptowährungen

5 Rechtliche Überlegungen zu Blockchain und einzelnen Anwendungen, insbesondere Kryptowährungen

Im Folgenden sollen einige Rechtsfragen eines Distributed Ledger mittels Blockchain behandelt werden. Ausgangspunkt der Betrachtungen ist ein vollständig dezentrales System. In hybriden oder zentral organisierten Systemen stellen sich viele der nachfolgend erörterten Fragen nicht oder nur teilweise. Dabei gibt es ein paar wenige Rechtsfragen, die sich allgemein für viele oder alle Blockchain-Anwendungen in dezentralen Systemen ergeben. Im Übrigen sind die sich aus der Blockchain-Technologie ergebenden rechtlichen Besonderheiten jeweils im Zusammenhang mit ihren Anwendungen zu betrachten. Je nach Anwendung (Zahlungsabwicklung, Abwicklung von Wertpapiertransaktionen, virtuelle Währungen, Dokumentenverwaltung, Register für Kfz oder – wenn nationale Rechte dies erlauben sollten – für Grundstücke, Markenrechte, Urheberrechte) stellen sich hier ganz eigene Fragen. Von dem Entstehen einer Lex Cryptographia zu sprechen,[57] erscheint demgegenüber mindestens stark verfrüht. Allerdings wird im Folgenden zu sehen sein, dass die dezentrale Organisation eines Distributed Ledger über die Blockchain dem deutschen Rechtssystem – und dies gilt für ausländische Rechtsordnungen gleichermaßen – bisweilen erhebliche Schwierigkeiten bereitet und auch für den Gesetzgeber bieten sich nicht immer einfache Lösungen und Strukturen, die privatrechtliche Ordnung und die öffentlichen Regulierungsanliegen in diesem Rahmen umzusetzen.

5.1 Allgemeine Rechtliche Fragen

Unabhängig von der einzelnen Anwendung der Blockchain stellen sich die Fragen der zivilrechtlichen Verantwortlichkeit, des wirksamen Vertragsschlusses im Rahmen von über DLT abgeschlossenen Transaktionen sowie insbesondere auch des Datenschutzes.

57 So aber Aaron Wright, Primavera De Filippi, »Decentralized Blockchain technology and the rise of Lex Cryptographia«. ↗ https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

5.1.1 Verantwortlichkeit

Prüfung von Transaktionen und Proof of Work

Eine Transaktion wird in der Blockchain durch einen Teilnehmer – es sind auch mehrere autorisierende Teilnehmer denkbar – ausgelöst, indem er die Transaktion mit seinem persönlichen Schlüssel (Signatur) autorisiert. Im Unterschied zu Intermediär-Modellen – wie Wertpapierhandel unter Beteiligung von Wertpapierhandelsbanken, Zahlungsabwicklung durch Zahlungsdienstleister oder Beurkundung von Transaktionen durch Notare – wird die Blockchain-Transaktion nach Autorisierung an einen Netzwerk-Knotenpunkt (network node) geschickt und über diesen an sämtliche anderen Netzwerk-Knotenpunkte, d. h. in das Blockchain-Netzwerk, (im Wege des broadcasting) übermittelt zwecks Validierung. Sobald einer der Netzwerk-Teilnehmer mit einem für die Validierung geeigneten Mining Netzwerk-Knotenpunkt (mining node) die Transaktion geprüft und für gut befunden hat, stellt dieser Teilnehmer (auch »Miner« genannt) sie zusammen mit einer bestimmten Anzahl anderer Transaktionen in einen Block ein und hängt sie der Kette anderer solcher Daten-Blöcke an, wodurch die Transaktion Teil der Blockchain wird.[58]

Die Miner können eine Vergütung für ihre Tätigkeit erhalten; in der Blockchain-Anwendung Bitcoin erhalten die Miner in der Regel eine in der Transaktion vom autorisierenden Teilnehmer inkludierte Transaktionsgebühr (i. d. R. ein Bruchteil eines Bitcoin) sowie gleichzeitig das Recht, weitere (neue) Bitcoins zu erstellen (im Wege des Mining = Schürfen). Die Vergütung erhält dabei derjenige, der als erster eine ausreichende Anzahl geprüfter Transaktionen in einen neuen (Candidate) Block einstellt, diesen Block abschließt und der Kette früherer Blocks, der Blockchain, hinzufügt.[59] Die anderen Miner, die dies auch versucht haben, gehen bei diesem Block leer aus.

Verantwortlichkeit des Miners

Zivilrechtlich stellt sich die Frage nach der Verantwortlichkeit des Miners für die Prüfung der einzelnen Transaktionen bzw. für den Proof of Work, insbesondere wenn sich im Laufe der Zeit herausstellt, dass die Transaktion doch nicht hätte validiert werden dürfen, weil z. B. der Rechner des Miners ein Double Spending übersehen hat. Dies kann bei einer Aktientransaktion darauf beruhen, dass der die Transaktion autorisierende Aktionär entweder dieselben Aktien zwei Mal verkauft und übertragen hat. Wird der Distributed Ledger mittels Blockchain für öffentliche Register, z. B. Kfz-Register (nach entsprechender Änderung des rechtlichen Rahmens), Markenregister, Grundbuch, Urheberrechtsregister u. ä., genutzt, so könnte es so sein, dass der ein Grundstück verkaufende Teilnehmer ein gar nicht auf ihn in der Blockchain eingetragenes Grundstück verkauft und überträgt.

In dem Fall könnte der Empfänger der Transaktion (z. B. der Aktien, des Grundstücks etc.) versuchen, einen Anspruch auf Schadenersatz gegen den Miner geltend zu machen, weil er (vielleicht)

58 Im Einzelnen Andreas M. Antonopoulos, Bitcoin & the Blockchain, Chapter 8, Mining and Consensus, abrufbar unter ↗ **https://chimera.labs.oreilly.com**, abgerufen am 01. September 2016.

59 Ausführlicher in Andreas M. Antonopoulos, a.a.O.

auf die Prüfung des Miners vertraut hat. Auch der Dritte könnte ggf. versuchen, Ansprüche gegen den Miner durchzusetzen, weil er die Verfügung eines Nichtberechtigten zugelassen hat. Die Ansprüche gegen den auslösenden Teilnehmer sollen hier nicht geprüft werden, weil sie nicht »Blockchain-typisch« sind.

Hier ist zunächst fraglich, ob eine Haftung des Miners gegenüber dem Empfänger der Transaktion aus Verletzung eines Vertrages in Betracht kommt. Der Name des Miners – erst recht nicht sein Sitz oder Aufenthalt – wird häufig nicht bekannt sein; die vom Teilnehmer eingesetzte Software vergibt jeweils Codes als Adressen des Teilnehmers. In dezentralen Systemen ist der Teilnehmer deshalb nicht notwendig namentlich identifizierbar,[60] so dass man hier von »Pseudonymität der Blockchain«[61] spricht. Allein deshalb ist bereits das anwendbare Recht für einen solchen (möglichen) Vertrag mit dem Miner schwer zu ermitteln. Ob ein Vertrag zwischen dem Miner und dem Empfänger der Transaktion angenommen werden kann, erscheint zweifelhaft, weil es dem Miner entscheidend um das Einkommen aus dem Miningprozess geht; dieses erzielt er zu einem Teil durch die Transaction Fees, die solche Teilnehmer zahlen, die eine Transaktion autorisieren. Das dürfte – wenn überhaupt – für einen Vertragsschluss allenfalls mit dem autorisierenden Teilnehmer sprechen. Ist solch ein Vertragsschluss das Ergebnis nach anwendbarem Recht, mag dieses auch den empfangenden Teilnehmer in den Schutzbereich des Vertrages einbeziehen; nach deutschem Recht erscheint das allerdings zweifelhaft. Selbst wenn man eine Haftungsgrundlage etablieren könnte, wäre das Verschulden nicht immer einfach nachzuweisen. Ist die eingesetzte Software des Miners selbst »lernfähig« und sind dabei entstehende Fehler für den Miner nicht vorhersehbar, dürfte dessen Verantwortlichkeit schwer zu begründen sein.[62]

5.1.2 Smart Contracts

Wenn vor allem Maschinen an einem Vertragsabschluss beteiligt sind, spricht man von »Smart Contracts«. Transaktionen in der Blockchain und damit zusammenhängende Leistungen basieren in der Regel auf automatisierten Abläufen, die die beteiligten Rechner mit Hilfe der darauf installierten Software und der Vorgaben des Nutzers selbst steuern. So ist über die Blockchain der sogenannte Computerhandel mit Wertpapieren denkbar, dem rechtlich eine Vielzahl von Kaufverträgen zugrunde liegt. Aber auch die zwischengeschalteten Tätigkeiten der Netzwerkteilnehmer, z. B. die Prüfungen durch die Miner, könnten – wie oben gesehen – Vertragsschlüsse über eben jene Prüfungstätigkeit beinhalten. Der Miner in der Blockchain lässt seinen Computer/sein Rechenzentrum nach ungeprüften Transaktionen und offenen Blocks der Blockchain

60 Andreas M. Antonopoulos Bitcoin & the Blockchain, Chapter 1, Introduction, abrufbar unter ↗ https://chimera.labs.oreilly.com, abgerufen am 01. September 2016.

61 Gerald Spindler/Martin Bille, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357, [●●●●]; Franziska Boehm, Paulina Pesch, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, Eine erste juristische Einordung, MMR 2014, 75 f.

62 Susanne Horner/Markus Kaulartz: Rechtliche Herausforderungen durch Industrie 4.0: Brauchen wir ein neues Haftungsrecht? – Deliktische und vertragliche Haftung am Beispiel »Smart Factory«, DSRITB 2015, 501.

suchen, lässt die Rechner eigenständig die Transaktionen prüfen und Blocks abschließen, um Transaction Fees einzunehmen.

Smart Contracts zeichnen sich dadurch aus, dass der Austausch von vertragskonstituierenden Willenserklärungen teilweise oder ganz über Maschinen erfolgt (z. B. ein intelligenter Kühlschrank bestellt eigenständig Milch, wenn der Vorrat zur Neige geht). Der Inhalt des Smart Contracts wird als Programmcode hinterlegt. Das vertragliche Pflichtenprogramm wird von einer Maschine automatisch ausgeführt, wenn die Voraussetzungen vorliegen, ohne dass eine unmittelbare menschliche Handlung erforderlich wäre. Gleichzeitig führt die automatisierte Durchsetzung dazu, dass im Fall von Missbrauch oder Verstößen gegen Vertragspflichten automatisiert die gewünschte Rechtsfolge ausgelöst wird – etwa eine Zugangs- oder Nutzungssperre, oder etwa finanzielle Sanktionen bzw. Beitragserhöhungen. Zahlt etwa ein Leasingnehmer die Leasingrate wiederholt nicht, so können im Leasingfahrzeug Technologien implementiert werden, die automatisiert eine Nutzungssperre auslösen. Smart Contracts können deshalb zukünftig dort eingesetzt werden, wo heute Intermediäre als Vertrauenspersonen tätig werden, d. h. beispielsweise Banken, Börsen, Treuhänder, Grundbuchämter oder auch Notare und ggf. Gerichtsvollzieher.

Vertragsschluss, Verbraucherrecht, Datenschutz

Smart Contracts stellen eine Herausforderung für das Rechtssystem dar. Exemplarisch zeigt sich dies unter anderem im Vertragsrecht, Verbraucherschutzrecht und Datenschutzrecht.

Hierbei ist zunächst zu klären, ob ein Vertragsschluss vorliegt, wenn die Maschine selbständig tätig wird oder gar an einem Bestellvorgang nur noch Maschinen beteiligt sind (M2M-Kommunikation). Nach deutschem Verständnis werden Erklärungen einer Maschine, bei denen der Nutzer vor Vertragsschluss wenigstens die Rahmenbedingungen (beispielsweise eine bestimmte Preisspanne, Auswahl an möglichen Vertragspartnern etc.) festlegt, grundsätzlich dem Nutzer der Maschine zugerechnet.[63]

Die Pseudonymität der Blockchain bereitet im Hinblick auf das anwendbare Recht und die Durchsetzbarkeit von vertraglichen Ansprüchen bei Smart Contracts Probleme, insbesondere wenn es um Online übermittelte bzw. genutzte Waren (Software, virtuelle Währungen, Bilder) oder Dienstleistungen geht. Der Verkäufer des Software-Updates, das meine Maschine, z. B. mein PC automatisch abruft, ist mir ggf. nicht erkennbar. Wenn man feststellt, dass das Software-Update Fehler hat, wird es schwer, Garantieansprüche durchzusetzen.

Wenn auf einer Seite solcher Smart Contracts Verbraucher beteiligt sind, hat der Unternehmer nach geltendem, weitestgehend EU-einheitlichem Recht dem Verbraucher vor Abgabe von dessen Vertragserklärung bestimmte Informationen zur Verfügung zu stellen und ihn über Widerrufsrechte zu belehren. Erfolgt jedoch der Vertragsschluss ausschließlich automatisiert, so stellt

63 Peter Bräutigam/Thomas Klindt, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137 ff.

sich einerseits die Frage, wie bzw. wo der Unternehmer die Informationen bereitstellen soll. Andererseits kann an der Zweckmäßigkeit der Informationspflichten gezweifelt werden, wenn der Verbraucher selbst die Informationen niemals ausliest, sondern dies rein maschinell erfolgt.[64]

Die Öffentlichkeit des dezentralen Distributed Ledger über die Blockchain wirft datenschutzrechtliche Fragen auf: Transaktionsdaten werden unter Verwendung von Pseudonymen öffentlich in der Blockchain hinterlegt und sind dort einsehbar. Wird das Pseudonym aufgedeckt (z. B. im Rahmen eines Hacker-Angriffs), kann auf Transaktionsdaten samt Identität der Person zugegriffen werden. Während die Verarbeitung der Daten im Rahmen des Vertragsverhältnisses i. d. R. durch die Abwicklung des vom Verbraucher gewünschten Vertrages gerechtfertigt ist, dürfte für die öffentliche Hinterlegung der Daten im Distributed Ledger eine besondere Einwilligung erforderlich sein.

5.2 Kryptowährungen im Rahmen der deutschen Finanzmarktregulierung

Besondere Fragen, insbesondere der öffentlichen Regulierung von Finanzdienstleistungen, stellen sich bei Ausgabe und Transfer von virtuellen Währungen wie Bitcoins oder Ether Coins, nachfolgend sogenannten Kryptowährungen. Sofern Kryptowährungen – wie von der Bank of England, von der niederländischen Zentralbanken und von anderen europäischen und außereuropäischen Zentralbanken beabsichtigt[65] – von einer Zentralbank ausgegeben werden, könnte die rechtliche Einordnung vollständig anders sein, weil und wenn es sich dabei um Zentralbankgeld handelt. Nur die dezentral (»privat«) geschaffenen Kryptowährungen wie Bitcoin werden nachfolgend als solche bezeichnet. Bei diesen stellt sich die grundlegende Frage, ob sie »Geld« im Rechtssinne sind und ob und inwieweit sie von der staatlichen Regulierung erfasst werden.

5.2.1 Ausgabe von Kryptowährungen im Rahmen der Geld-Regulierung

Zunächst ist festzustellen, dass es weder im deutschen noch im Europarecht einen einheitlichen Geldbegriff gibt. Vielmehr werden die Begriffe »Geld« und »Zahlungsmittel« je nach Normenkomplex unterschiedlich interpretiert (relativer Geldbegriff).

64 Zum Ganzen Peter Bräutigam/Thomas Klindt, a.a.O.

65 BoE, Staff Working Paper No. 605 »The macroeconomics of central bank issued digital currencies« (↗ http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf).

Dezentrale nicht hoheitliche Kryptowährungen sind kein Zentralbankgeld

Nach § 35 Abs. 1 BBankG ist strafbar, wer unbefugt Geldzeichen oder unverzinsliche Inhaberschuldverschreibungen ausgibt, auch wenn ihre Wertbezeichnung nicht auf Euro lautet. Mit Geldzeichen gemeint sind hier jedoch die von einer Zentralbank ausgegebenen, gesetzlichen Zahlungsmittel und nicht Marken, Münzen oder Scheine einer privaten Währung, die nicht die Eigenschaft eines gesetzlichen Zahlungsmittels hat.[66] Die Ausgabe einer solchen privaten Währung ist nicht nach § 35 Abs. 1 BBankG verboten.

Dezentrale nicht hoheitliche Kryptowährungen sind nicht E-Geld

Dezentral nicht hoheitlich ausgegebene Kryptowährungen sind auch nicht E-Geld im Sinne von § 1 a Abs. 3 ZAG bzw. der zugrunde liegenden Zweiten E-Geld-Richtlinie. Dabei ist E-Geld ein elektronisch, darunter auch magnetisch, gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge im Sinne des § 675f Absatz 3 Satz 1 des Bürgerlichen Gesetzbuchs durchzuführen und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird.

Obschon es sich bei dezentral, nicht hoheitlich ausgegebenen Kryptowährungen um elektronisch gespeicherte und monetäre Werte handelt, fehlt es ihnen für die Qualifikation als E-Geld an einer Forderung gegen einen Emittenten. Aufgrund der Tatsache, dass es keinen zentralen Emittenten gibt, verpflichtet sich auch niemand zur Einlösung oder zum Rücktausch dieser Kryptowährung.[67] Darüber hinaus werden sie nicht gegen Zahlung eines Geldbetrages[68] ausgegeben, sondern durch Mining geschaffen, d. h. durch Einsatz von Rechenleistung zur Lösung einer komplizierten mathematischen Aufgabe.

Dezentrale nicht hoheitliche Kryptowährungen sind kein Zahlungsmittel im Sinne des Zivilrechts

Ob dezentrale nicht hoheitliche Kryptowährungen Geld im Sinn des deutschen Zivilrechts darstellen, so dass damit Geldschulden erfüllt werden könnten und der Gläubiger gezwungen wäre, diese Kryptowährungen als Erfüllung anzunehmen, erscheint zweifelhaft.

Gesetzliches Zahlungsmittel zur Erfüllung einer Geldforderung nach dem BGB ist in Deutschland seit dem 01. Januar 2002 der Euro. Dabei ist streitig, ob eine Geldschuld sowohl in Bargeld

66 Jan Luckey, Ein europarechtlicher Rahmen für das elektronische Geld, WM 2002, 1529.

67 RegBegr. Zweite E-Geld-RLUG, BT-Drucks. 17/3023, S. 40; BaFin-Merkblatt v. 22. Dezember 2011, Hinweise zum Zahlungsdiensteaufsichtsgesetz, Abschn. 4.b; Michael Findeisen in Ellenberger/Findeisen/Nobbe, § 1a ZAG Rn. 55: »E-Geld im technischen Sinne«; Matthias Terlau, in: Casper/Terlau, ZAG, 1. Aufl. 2014, § 1a Rn. 50.

68 Geld im Sinn der Zweiten E-Geld-Richtlinie und der Zahlungsdiensterichtlinie ist dabei Bargeld, Buchgeld oder E-Geld: Vgl. Art. 4 Nr. 15 Zahlungsdiensterichtlinie.

als auch in Buchgeld erfüllt werden kann. Bargeld sind verkörperte Geldzeichen, die in einer Rechnungseinheit gestückelt sind, einen Nominalwert aufweisen und als Zahlungsmittel staatlich anerkannt sind. Dezentrale nicht hoheitlichen Kryptowährungen fehlt es sowohl an der Verkörperung, als auch an einer staatlichen Anerkennung, sodass es sich dabei nicht um Bargeld handelt. Da derartige Kryptowährungen keine Forderung gegen ein Kreditinstitut oder sonst jemanden verkörpern, verbriefen oder beinhalten, handelt es sich auch nicht um Buchgeld.

Die Vereinbarung der »Bezahlung mit Bitcoins« stellt deshalb keine Vereinbarung einer Geldschuld im Sinne des deutschen Zivilrechts dar[69] und gesetzliche Geldschulden können nicht mit diesen beglichen werden. Die Vereinbarung der »Bezahlung mit Bitcoins« stellt vielmehr zivilrechtlich ein Tauschgeschäft im Sinn des § 480 BGB dar. Der Tauschvertrag auf den kaufvertragliche Regelungen entsprechend anzuwenden sind, ist deshalb bei einer Bezahlung von Waren mit dezentrale nicht hoheitlichen Kryptowährungen wie Bitcoins der richtige Vertragstypus.

5.2.2 Handel mit virtuellen Währungen im Bankaufsichtsrecht

Sollte es sich bei dezentralen nicht hoheitlichen Kryptowährungen um Finanzinstrumente handeln, wäre ihre Vermittlung sowie ihr Handel und Umtausch im Inland, nicht jedoch Ausgabe und Schaffung, der deutschen Finanzaufsicht unterworfen. Infolge dessen bestünde für Dienstleister die gewerbsmäßig oder in einer einen kaufmännisch eingerichteten Geschäftsbetrieb erfordernden Weise mit solchen Kryptowährungen handeln und einen der Tatbestände des § 1 Abs. 1 oder Abs. 1a KWG erfüllen ein strafbewehrtes Verbot mit Erlaubnisvorbehalt gemäß § 32 Abs. 1 KWG für ihre Tätigkeit im Inland.

Kryptowährungen als Finanzinstrumente

Nach Ansicht der deutschen Finanzaufsicht BaFin[70] und der herrschenden Meinung handelt es sich bei dezentralen nicht hoheitlichen Kryptowährungen um Rechnungseinheiten und Finanzinstrumente im Sinne des § 1 Abs. 11 S. 1 Nr. 7 Alt. 2 KWG.

Eine Definition des Begriffs »Rechnungseinheit« wird zwar weder durch das Gesetz noch durch Rechtsprechung oder Literatur geliefert. Da der Begriff in den nationalen Aufsichtsrechten verschiedener anderer EU-Mitgliedstaaten nicht zur Verfügung steht, weicht die deutsche aufsichtsrechtliche Einordnung von der Rechtspraxis vieler EU-Mitgliedstaaten ab. Auch hatte man bisher bei Recheneinheiten im Sinne dieser Vorschrift eher die Sonderziehungsrechte des Inter-

69 Offener Gerald Spindler/Martin Bille, WM 2014, 1357, 1361: »Grundsätzlich können dem Bitcoin die Geldfunktionen nicht abgesprochen werden.«; anders auch Benjamin Beck, Bitcoins als Geld im Rechtssinne, NJW 2015, 580, 585: können bei entsprechender Parteiabrede grundsätzlich Leistungsgegenstand einer Geldschuld sein.

70 BaFin-Merkblatt v. 22. Dezember 2011, Hinweise zum Zahlungsdiensteaufsichtsgesetz, Abschn. 4.b; BaFin-Merkblatt v. 20.12.2011 (Stand Juli 2013), Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 S. 1 Nr. 1 bis 7 KWG, Abschn. 2.b.hh); Michael Findeisen in Ellenberger/Findeisen/Nobbe, § 1a ZAG Rn. 55: »E-Geld im technischen Sinne«; vgl. auch Jens Münzer, BaFin Journal 2014, 26, 27.

nationalen Währungsfonds[71] und den ECU (European Währung Unit) vor Augen. Dabei handelt es sich jedoch um Einheiten, die auf staatliche Währungen Bezug nehmen. Die Einordnung von dezentralen nicht hoheitlichen Kryptowährungen wie z. B. Bitcoins als Rechnungseinheit ist demgemäß nicht zweifelsfrei.

Es dürfte aber die Notwendigkeit des Schutzes der Öffentlichkeit vor Missständen der Finanzwirtschaft, insbesondere des Geldverkehrs, dafür sprechen, derartige Kryptowährungen als Rechnungseinheit einzuordnen und damit den Handel mit diesen einer eingeschränkten Finanzaufsicht zu unterwerfen.[72] Bitcoins und zunehmend auch andere Kryptowährungen haben aufgrund ihrer aktuell relativ verbreiteten Akzeptanz im weltweiten Online- und teilweise auch im Offline-Handel eine gewisse Bedeutung als Tauschmittel erlangt und erfüllen in der Praxis volkswirtschaftlich Geldfunktionen. Des Weiteren werden sie als Wertaufbewahrungsmittel eingesetzt.

Einzelne Tätigkeiten im Zusammenhang mit Kryptowährungen

Wegen der Qualifikation von dezentralen nicht hoheitlichen Kryptowährungen als Finanzinstrument sind bestimmte Bank- oder Finanzdienstleistungen, die im Inland erbracht werden, der Erlaubnispflicht unterworfen. Dabei gilt der »weite Inlandsbegriff«, wonach es ausreicht, dass vom Ausland mit Mitteln der modernen Kommunikation gezielt Kunden im Inland angesprochen werden und Teilakte der aufsichtspflichtigen Tätigkeit im Inland verwirklicht werden.[73] Internetplattformen, die vom Ausland aus betrieben werden, können deshalb den Inlandsbegriff erfüllen und einer Erlaubnis durch die BaFin bedürfen, wenn sie gezielt (auch) den deutschen Markt ansprechen.

Eine Erlaubnis ist aber dann nur erforderlich, wenn die Dienstleistung gewerbsmäßig oder einen kaufmännischen Geschäftsbetrieb erfordernd angeboten wird. Wer also derartige Kryptowährungen kauft, um sie lediglich zur Bezahlung zu verwenden, ist im Rahmen der deutschen Regulierung erlaubnisfrei.

Kryptowährungs – Tausch- und Wechselgeschäfte

Sofern jemand dezentrale nicht hoheitliche Kryptowährungen an- und verkauft und dies als Dienstleistung Dritten anbietet, kommt der Tatbestand des Eigenhandels § 1 Abs. 1a S. 2 Nr. 4 lit. a) bis c) KWG in Betracht.

71 Gesetzesbegründung zum Finanzmarkt-Richtlinie-Umsetzungsgesetz.

72 Gerald Spindler/Martin Bille, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357 ff.

73 BVerwG WM 2009, 1553, 1557 ff. Rn. 36.

Nach dem Auffangtatbestand des § 1 Abs. 1a S. 2 Nr. 4 lit. c) KWG ist Eigenhändler wer Finanzinstrumente im eigenen Namen und auf eigene Rechnung als Dienstleistung kauft oder verkauft. Charakteristisch ist regelmäßig ein, durch den besseren Zugang des Eigenhändlers zum Markt bewirktes, Ungleichgewicht zwischen Eigenhändler und Kunden.[74]

Mining-Pools

Im Fall von Mining-Pools, bei denen sich mehrere derartige Kryptowährungs-Teilnehmer zusammenschließen und anschließend die geschürfte Menge an Kryptowährung veräußern, kann bei dem Teilnehmer der dies organisiert aufgrund des in der Veräußerung enthaltenen Dienstleistungselements, Eigenhandel im Sinn von § 1 Abs. 1a S. 2 Nr. 4 lit. c) KWG vorliegen. Je nach Ausgestaltung können deshalb Betreiber oder Initiatoren von Mining Pools den Tatbestand des Eigenhandels, des Platzierungsgeschäfts oder der Abschlussvermittlung erfüllen.

Handelsplattformen für Kryptowährungen

Plattformen, auf denen Dritte Kryptowährungen handeln können, erfüllen – je nach Ausgestaltung – die Tatbestände des Finanzkommissionsgeschäfts gemäß § 1 Abs. 1 S. 2 Nr. 4, der Anlagenvermittlung gemäß § 1 Abs. 1a S. 2 Nr. 1 KWG, der Abschlussvermittlung gemäß § 1 Abs. 1a S. 2 Nr. 2 KWG oder des Betriebs eines multilateralen Handelsplattform gemäß § 1 Abs. 1a S. 2 Nr. 1b KWG. Erlaubnispflichtig sind sie, wenn die Tätigkeit gewerbsmäßig oder in einer Art erfolgt, die einen kaufmännischen Geschäftsbetrieb erfordert. Richten sich Handelsplattformen an inländisches Publikum, ist deshalb jeweils im Einzelfall zu prüfen, welcher der Tatbestände einschlägig sein kann.[75]

Anbieter von Kryptowährungs-Wallets

Anbieter von Online Wallets, in denen Kryptowährungs-Teilnehmer ihre privaten Schlüssel speichern können, sind nach dem KWG nicht erlaubnispflichtig, da kein Einlagengeschäft (§ 1 Abs. 1 S. 2 Nr. 1 KWG), kein Depotgeschäft (§ 1 Abs. 1 S. 2 Nr. 5 KWG, kein Finanzkommissionsgeschäft und keine Finanzportfolioverwaltung (§ 1 Abs. 1a S. 2 Nr. 3 KWG) vorliegt. Da sich sämtliche Tatbestände des Zahlungsgeschäfts im Sinn von § 1 Abs. 2 ZAG auf den Transfer oder den Zugang zu Geld im Sinn von Art. 4 Nr. 15 Zahlungsdiensterichtlinie, namentlich Bargeld, Buchgeld oder E-Geld beziehen und dezentrale nicht hoheitliche Kryptowährungen unter keinen dieser Geldbegriffe fallen, sind Kryptowährungs- Online Wallets weder nach dem KWG noch nach dem ZAG erlaubnispflichtig.

74 BaFin-Merkblatt vom 22.3.2011 (Stand Oktober 2014),
Merkblatt – Hinweise zu den Tatbeständen des Eigenhandels und des Eigengeschäfts, Abschn. 2.b).

75 Jens Münzer, BaFin Journal 2014, 26, 29.

Mining

Die Erstellung neuer Bitcoins durch Lösen komplexer mathematischer Rechenaufgaben stellt keine nach dem KWG regulierte Tätigkeit dar, weil die Schaffung von Rechnungseinheiten im Sinn des § 1 Abs. 11 S. 1 Nr. 7 Alt. 2 KWG nicht von einem Tatbestand des § 1 Abs. 1 oder Abs. 1a KWG erfasst ist.[76]

5.3 Crowdfunding, -lending, Zahlungsabwicklung und Wertpapierhandel über die Blockchain

Regulatorisch ergeben sich vielfältige Probleme bei Abwicklung von Finanztransaktionen mittels Distributed Ledgers über die Blockchain. Insbesondere erlaubt die Blockchain-Technologie die Abwicklung einer Transaktion von Gütern (Geld, Wertpapiere, Grundstückseigentum) ganz ohne Dritte, die in die Dokumentation, in die Feststellung der Parteien und der gegenseitigen Forderungen der beteiligten Parteien (Clearing) und in die Gewährleistung der Zug-um-Zug-Abwicklung (Settlement) eingeschaltet werden.

5.3.1 Anknüpfung an den Intermediär, globale Abwicklung

Im Grundsatz knüpft das deutsche und europäische Finanzaufsichtsrecht (vielfach) bei den Intermediären (Einlagen oder Krediten das Kreditinstitut, bei Wertpapierhandel das Wertpapierdienstleistungsunternehmen und Clearingstell(en), bei Zahlungsabwicklung der Zahlungsdienstleister und/oder die Clearingstelle) an. Diese sind die von der Finanzaufsicht (in Deutschland die BaFin) beaufsichtigen Institute. In einem dezentralen System, wie sie ein Distributed Ledger über die Blockchain darstellt, sind die herkömmlichen Intermediärs-Funktionen jedenfalls nicht anzutreffen.

Blockchain ist ein weltweites Phänomen. Häufig ist es für eine Teilnahme auch nicht erheblich, wo jemand sich gerade aufhält. Die deutsche Finanzaufsicht ist aber nur berufen, wenn Bank-, Finanzdienstleistungs- Zahlungs- oder E-Geld-Geschäfte »im Inland« erbracht werden. Dafür ist mindestens erforderlich, dass vom Ausland mittels Telekommunikationsmedien wesentliche zum Vertragsschluss hinführende Schritte im Inland vorgenommen werden sollen, in der Regel reicht eine zielgerichtete Ansprache inländischer Kunden.[77] Es reicht nicht, wenn der Kunde auf eigene Initiative Dienstleistungen eines ausländischen Unternehmens nachfragt, dessen Angebot sich nicht (auch) an eine inländische Zielgruppe richtet.[78]

76 BaFin-Merkblatt v. 22.12.2011, Hinweise zum Zahlungsdiensteaufsichtsgesetz, Abschn. 4.b; Münzer, BaFin Journal 2014, 26, 27; zustimmend Spindler/Bille, WM 2014, 1357, 1364.

77 BVerwG WM 2009, 1553, 1557 ff. Rn. 36.

78 BVerwG a.a.O. Rn. 47.

5.3.2 Crowdfunding – Einlagengeschäft über Blockchain

Das Einsammeln von Einlagen über die Blockchain wirft regulatorisch keine Besonderheiten auf. Einlagen sind jedenfalls von der deutschen und der europäischen Regulierung nur dann erfasst, wenn ihnen staatliches Bargeld oder Buchgeld zugrunde liegt. E-Geld sollte auch unter den Geldbegriff des Einlagentatbestands fallen.[79] »Virtuelle« Währungen, insbesondere Bitcoins, dagegen nicht.[80]

Verwaltung von Geldern in der Blockchain ist für jedermann einsehbar. Das ist bei Bitcoins (die keine Einlagen darstellen) derzeit schon der Fall. Will eine Bank solche Guthabenkonten – für jedermann einsehbar – über den Distributed Ledger verwalten, müsste sie sich zunächst vom Bankgeheimnis entbinden lassen. Auch das allgemeine Datenschutzrecht ist zu beachten.

5.3.3 Crowdlending – Kreditgeschäft über die Blockchain

Auch bei Krediten, die über die Blockchain abgewickelt werden, stellen sich nur wenige Besonderheiten. Die Vergabe von Krediten ist in Deutschland den Kreditinstituten vorbehalten, wenn sie gewerbsmäßig oder in einem Umfang erfolgt, der einen kaufmännisch eingerichteten Geschäftsbetrieb erfordert. Soll die Vergabe und Abwicklung über DLT stattfinden, wäre die Bank vorher wirksam vom Bankgeheimnis zu entbinden.

Je nach Struktur der vermittelten Kredite und der Refinanzierung der Kredite kann dabei die Vermittlungsplattform eine Erlaubnis nach dem KWG als Anlagevermittler benötigen;[81] auch das ist nicht spezifisch für mit Blockchain-Technologie, sondern würde auch beim Einsatz anderer Technologien für die Vermittlungsplattform gelten.

5.3.4 Zahlungstransaktionen über die Blockchain

Banken, spezialisierte undweltweit tätige Zahlungsdienstleister wie MoneyGram oder Western Union, zahlreiche Zahlungsinstitute und E-Geld-Institute wie u. a. PayPal wickeln Geldtransfers für ihre Kunden ab. Sie benötigen hierfür – je nach Geschäftsmodell und Land ihrer Tätigkeit – unterschiedliche Erlaubnisse der nationalen Aufsichtsbehörden. In jüngster Zeit werden Systeme getestet, mit denen Zahlungen über Blockchain-Technologie transferiert werden.[82] Dabei mag es so sein, dass zunächst nur die Benachrichtigung über die Zahlung (ähnlich wie bei

79 Frank A. Schäfer, in: Boos/Fischer/Schulte-Mattler, KWG, CRR-VO, 5. Aufl. 2016, § 1 Rn. 37.

80 BaFin, Merkblatt – Hinweise zu Finanzinstrumenten nach § 1 Abs. 11, Stand: 7/2013, S. 10; Spindler/Bille, WM 2014, 1357 (1361 mwN); Beck, NJW 2015, 280 ff.; Lerch, ZBB 2015, 190 ff.

81 Vgl. die Meldung: Bitcoin-Kreditplattform Bitbond bekommt BaFin-Lizenz vom 13. Oktober 2016, ↗ http://www.heise.de/newsticker/meldung/Bitcoin-Kreditplattform-Bitbond-bekommt-BaFin-Lizenz-3347905.html

82 Vgl. Pressemitteilung der Reisebank AG vom 19. Juli 2016, ↗ http://www.presseportal.de/pm/116526/3382017

SWIFT) über den auf Blockchain-Technologie basierenden Distributed Ledger transferiert wird; bei Fortentwicklung mag auch der Transfer des Guthabens selbst über die Blockchain gelingen.

Beim Geldtransfer keine Zahlungsdienstleister beteiligt

Bei dezentraler Abwicklung von Zahlungstransaktionen über DLT sind Zahlungsdienstleister und Clearing- und Settlement-Stellen für Zahlungsvorgänge nicht mehr erforderlich. Die zu transferierenden Gelder (Buchgeld, E-Geld) würden auch nicht von einer sonstigen dritten, am Zahlungsvorgang nicht beteiligten Parteien entgegengenommen, verwaltet und versandt, sondern nur von den beiden Parteien. Gleichzeitig bedeutet dies eine nahezu zeitgleiche Abwicklung jeder Zahlungstransaktion. Zum Vergleich: Die Validierung einer Transaktion in Bitcoins dauert derzeit ca. 10 Minuten.[83]

Validierung der Transaktionen durch Miner

Als Dritte sind an der einzelnen Transaktion nur die Miner beteiligt. Der Miner erhält dabei – unterstellt es handelt es sich um ein dezentrales DLT-System entsprechend dem Bitcoin-System – zwar keinen Zugriff auf das zu transferierende Buch- oder E-Geld. Er prüft vor allem die Schlüssigkeit der Transaktionsdaten in sich und anhand der von dem auf Blockchain-Technologie basierenden Netzwerk vorgegebenen Kriterien, er prüft die Berechtigung des Zahlers anhand früherer Transaktionen, er prüft, ob weitere Transaktionen über denselben »Output« oder Bruchteile hiervon vorliegen etc.[84] Damit aber üben die Miner die wichtigste Funktion in der Blockchain aus. Fehler oder Missbrauch bei den Minern kann zum Zusammenbruch des Systems führen.

Miner sind von der aktuellen Regulierung nicht erfasst

Allerdings würde der Miner (selbst wenn er im Inland seinen Sitz hätte) wohl nicht als Zahlungsdienstleister von der aktuellen Zahlungsregulierung (dem deutschen Ausführungsgesetz zur PSD1 oder von der PSD2) erfasst. Sie erbringen keine Zahlungsdienste im Sinn der Definitionen der der PSD1 oder PSD2. Dem Miner kommt lediglich die Funktion eines außen stehenden Gutachters bzw. Schiedsrichters über die Richtigkeit der Transaktion zu.

Änderung der Zahlungsregulierung erforderlich

Wollte man den Miner der Regulierung unterwerfen, müsste der europäische Gesetzgeber die gerade in Form der PSD2 neu gefasste Zahlungsdiensterichtlinie erneut ändern. Eine Vorlage für entsprechende Gesetze (zu Bitcoins) haben die US-Bundesstaaten New York im Jahr 2015[85] und

83 Andreas M. Antonopoulos, Bitcoin & the Blockchain, Chapter 8, Mining and Consensus, abrufbar unter ↗ **https://chimera.labs.oreilly.com**, abgerufen am 01. September 2016.

84 Im Einzelnen Andreas M. Antonopoulos, a.a.O.

85 ↗ **https://www.cryptocoinsnews.com/final-new-york-bitcoin-regulation-released-bitlicense**; vgl. hierzu Matthias Terlau, Bitcoins Regulierung – Was steckt in der viel diskutierten »Virtual Währungen Regulation« des US-Bundesstaates New York?, in ↗ **http://payment-law.eu** vom 01. September 2014.

North Carolina in 2016[86] geliefert; der Bundesstaat Washington (das ist nicht Washington D.C.) könnte bald folgen. Die auf Blockchain-Zahlungstransaktionen spezialisierten Unternehmen Ripple Labs, Inc. und Circle Internet Financial Inc. haben bereits eine New Yorker BitLicense erworben.[87] Aus Sicht der regulatorischen Zielsetzung der Sicherheit des Zahlungssystems und der Geldwäscheprävention mag eine solche Regulierung durchaus wünschenswert sein.[88] Von den sich gerade entwickelnden Unternehmen mit Geschäftsmodellen rund um die Blockchain werden solche Regulierungen als Hemmschuh im Rahmen der Entwicklung und Erprobung sinnvoller Anwendungen angesehen.[89]

5.3.5 Zahlungsabwicklung, Geldwäsche- und Sanktionsrecht

Der Gesetzgeber will im Rahmen der Regulierung des Zahlungsverkehrs zugleich die regulierten Parteien in (s)ein System der Geldwäscheprävention und Bekämpfung der Terrorismusfinanzierung einbinden. Ziel des Gesetzgebers des Geldwäscherechts ist es, eine »Papierspur« der transferierten Gelder sicher zu stellen.[90] Hinzu kommen im Regelfall einer Zahlungstransaktion zusätzlich verschiedene Prüfungen nach nationalen und überregionalen Sanktionsrechten (Sanction Screening).

Miner wären nicht Verpflichtete nach Geldwäscherecht

Vom deutschen Geldwäscherecht wäre der Miner nicht erfasst. Er ist weder Institut noch ist er Agent oder Vertriebsunternehmen von Instituten. Weltweit müsste vermutlich die jeweils nationale Geldwäschegesetzgebung angepasst werden, wollte man die Zahlungsströme über die Blockchain erfassen.[91]

Pseudonymität und Identifizierung nach Geldwäscherecht

Geldwäscherechtlich stünde aber zum einen die Pseudonymität der Blockchain einer effizienten Geldwäscheprüfung entgegen. Zahler und/oder Zahlungsempfänger müssten ihre Pseudonymität Preis geben. Hier stellt sich bereits die Frage, wem gegenüber dies erfolgen sollte, d. h. wer soll Verpflichteter der geldwäscherechtlichen Identifizierungs- und Prüfungspflichten sein. Man könnte erwägen, dass jeder Teilnehmer der Blockchain seine zur Identifizierung benötigten Daten in der Blockchain ablegt. Mit einem solchen Gedanken spielt offenbar die EU Kommission

86 ↗ http://www.coindesk.com/north-carolina-governor-signs-bitcoin-bill-law

87 ↗ http://www.coindesk.com/circle-granted-first-bitlicense-rebrands-as-circle-pay
↗ https://ripple.com/insights/ripple-receives-new-yorks-first-bitlicense-institutional-use-case-digital-assets

88 Zu den Zielsetzungen der europäischen Zahlungsregulierung vgl. Matthias Terlau, ZBB 2016, 122 ff.

89 ↗ http://www.coindesk.com/new-york-bitcoin-scene-divided-as-bitlicense-deadline-looms

90 Entwurf der Bundesregierung zum Gesetz zur Umsetzung der 3. Geldwäscherichtlinie, BT-Drucks 16/9038, S. 29; vgl. zu den geldwäscherechtlichen Zielen der Zahlungsregulierung auch Matthias Casper/Matthias Terlau, in: Casper/Terlau, ZAG, 1. Aufl. 2014, Einleitung Rn. 11.

91 Vgl. hierzu die geldwäscherechtlichen Regelungen der New Yorker Bitcoin-Regulierung, oben Fn. 86.

in ihrem jüngsten Vorschlag vom 5.7.2016 zur Änderung der 4. Geldwäscherichtlinie.[92] Das dürfte aber kein praktikabler Weg sein, wenn diese Daten dann öffentlich einsehbar wären; das würde sich wohl aus Datenschutzgründen verbieten. Für den einzelnen Verbraucher, der sich dann selbst identifizieren und überprüfbare Nachweise seiner Identität hinterlegen soll, dürfte erschwerend wirken, dass es keinen (europaweit[93] oder weltweit) einheitlichen Standard der Angaben zur Identifizierung und der Art und Weise der Prüfung der Angaben der identifizierten Person gibt.

Verpflichteter zur Durchführung der Identifizierung

Kommt eine Hinterlegung der Identifizierungsdaten des Zahlers/Zahlungsempfängers in der Blockchain nicht in Betracht, so benötigt man eine identifizierende Person. Wollte man den Miner zur geldwäscherechtlichen Identifizierung verpflichten, würden sich zahlreiche weitere Fragen stellen.

Der Miner müsste wohl das nationale Geldwäscherecht des Staates beachten, in dem er seinen Sitz oder seine Niederlassung hat. Für den Miner würden derartige Pflichten einen hohen Verwaltungsaufwand nach sich ziehen.

Zudem wäre es für ihn bereits nicht einfach – auch wegen der Pseudonymität der Blockchain-Teilnehmer – herauszufinden, welche Rechtsordnungen im konkreten Fall beteiligt sein können.

Des Weiteren stellt sich die Frage nach dem geeigneten Zeitpunkt der Identifizierung. Die Prüfung der Transaktion wird – im Wettrennen der Miner – üblicherweise von einer großen Vielzahl von Minern durchgeführt. Es ist kaum vorstellbar, jeden dieser (in Wettstreit tretenden) Miner zur Identifizierung des Zahlers/Zahlungsempfängers zu verpflichten. Zudem stellt sich die Frage, ob jeweils beide an der Transaktion beteiligten Parteien identifiziert werden müssten.

Staatliches Sanktionsrecht erfasst häufig bereits den Miner

Nach staatlichem Exportkontrollrecht kann es verboten sein, bestimmten Personen Geldbeträge zur Verfügung zu stellen.[94] Neben den Parteien sind auch Zahlungsdienstleister i. d. R. verpflichtet, solch staatliches Sanktionsrecht zu beachten, z. B. Gelder einzufrieren oder jedenfalls die Einhaltung von staatlichem Sanktionsrecht zu kontrollieren.[95] Diese Pflichten würden auch einen Miner treffen.

92 Vgl. COM(2016) 450 final, 2016/0208 (COD), S. 9.

93 Die 4. Geldwäscherichtlinie bringt ja – ebenso wie die Vorgänger-Richtlinie – nur eine Mindestharmonisierung und lässt den Mitgliedstaaten sehr viel Freiraum für unterschiedliche Identifizierungs- und Überprüfungsregelungen.

94 Vgl. z. B. Art. 2 (2) der Verordnung (EU) Nr. 359/2011 vom 12. April 2011 (Iran): »Den in Anhang I aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugute kommen.«

95 Andrea Hügle, in: Ehlers/Wolffgang, Recht der Exportkontrolle, 2015, S. 577.

5.3.6 Abwicklung von Wertpapiertransaktionen über die Blockchain

Denkbar sind Handelssysteme für Aktien- und sonstigen Wertpapierhandel über Blockchain. Vor allem Prozesse zur Abwicklung außerbörslich gehandelter Wertpapiere werden auf Einsatzmöglichkeiten der Blockchain untersucht.[96] Auch hier werden die Transaktionen über den Konsens der Netzwerkteilnehmer verifiziert. Dabei sollen die Abwicklungszeiten, -kosten und -risiken des außerbörslichen Wertschriftenhandels minimiert werden; Lieferung und Zahlung des Wertpapiers soll im besten Fall »real-time« erfolgen.

Eine Herausforderung dabei ist, dass das Trading-Reporting den regulatorischen Anforderungen entspricht. Zu den möglichen Teilnehmenden einer solchen Blockchain-basierten Handelsplattform gehören auch die Aufsichtsbehörden, die damit eine Missstandsaufsicht unmittelbar in der Blockchain übernehmen könnten.

Regulatorische Leitplanken

Für übertragbare Wertpapiere, die an Handelsplätzen im Sinn der MiFiD gehandelt werden, gilt nach der CSDR[97] ab 01. Januar 2023 (bei Neuemissionen) bzw. ab 01. Januar 2025 (für alle Wertpapiere), dass sie bei einem Zentralverwahrer im Effektengiro eingebucht werden müssen, damit unter anderem gewährleistet ist, dass sie in einem Wertpapierliefer- und -abrechnungssystem abgewickelt werden können.[98] Erfasste Handelsplätze sind neben geregelten Märkten, auch organisierte Handelssysteme und multilaterale Handelssysteme.[99] Damit bleiben nur wenige Anwendungsfälle, in denen die Pflicht zur Hinterlegung nach der CSDR nicht eingreift.

Damit hat auch eine Abwicklung über die Blockchain zunächst von der Zentralverwahrung auszugehen. Eine Ausgabe übertragbarer Wertpapiere (in dematerialisierter Form) unmittelbar über die Blockchain – ohne Hinterlegung bei einem Zentralverwahrer – ist dann (ohne Änderung des europäischen Rechts) praktisch nicht zulässig.

Die Hinterlegungspflicht bedingt aber wohl – das ist der CSDR nicht mit Bestimmtheit zu entnehmen – nicht gleichzeitig eine Clearing- und Settlement-Pflicht über einen Zentralverwahrer für sämtliche übertragbaren Wertpapiere. Denkbar wäre deshalb, dass die buchmäßige Verwahrkette vom Effektengiro des Zentralverwahrers in die Blockchain übergeleitet und dort im

96 Basis für außerbörslich gehandelte Aktien – Blockchain, business24.ch vom 09. September 2016.

97 Verordnung (EU) Nr. 909/2014 des Europ. Parlaments u. des Rates v. 23.7.2014 zur Verbesserung der Wertpapierlieferungen u. -abrechnungen in der EU u. über Zentralverwahrer, ABl. 2014 L 257, ABLEU 2014 L Seite 1.

98 Art. 3 Abs. 1 CSDR mit Erwägungsgrund 11.

99 Art. 4 Nr. 24 MiFiD II.

DL-Verfahren fortgeführt wird. Clearing ist nur bei den der EMIR[100] unterfallenden OTC-Derivatekontrakten[101] verpflichtend.

Zulassungspflicht für Handelsplätze

Handelsplätze sind neben geregelten Märkten, auch organisierte Handelssysteme und multilaterale Handelssysteme. Der Betrieb eines geregelten Marktes ist zulassungspflichtig.[102] Bereits heute ist infolge MiFiD I der Betrieb einer multilateralen Handelsplattform als Finanzdienstleistung zulassungspflichtig.[103] Nach MiFiD II[104] sind der Betrieb eines organisierten Handelssystems und der Betrieb eines multilateralen Handelssystems jeweils zulassungspflichtige Wertpapierdienstleistungen und Anlagetätigkeiten.

Der Betreiber eines mit Distributed Ledger über Blockchain abgewickelten Wertpapier-/Finanzinstrumente-Handels wird also in Zukunft in den meisten Fällen der Erlaubnis der BaFin bedürfen. Die Zulassungspflicht läuft allerdings dann u. U. leer, sofern es sich um ein wahrhaft dezentrales System handelt, das keine Betreiber, sondern nur Netzwerkteilnehmer hat.

Die aktuelle Regulierung von multilateralen Handelsplattformen erfasst den Betreiber dann, wenn »die Interessen einer Vielzahl von Personen am Kauf und Verkauf von Finanzinstrumenten innerhalb des Systems und nach festgelegten Bestimmungen in einer Weise zusammengebracht werden, die zu einem Vertrag über den Kauf dieser Finanzinstrumente führt«.[105] Die Teilnehmer an einem DLT basierten Wertpapierhandel bringen aber nicht selbst eine Vielzahl von Personen zusammen; weder die Teilnehmer, die Wertpapiere dort anbieten oder abnehmen, noch diejenigen Teilnehmer, die Mining-Netzwerkknotenpunkte unterhalten (»Miner«), sind in diesem Sinn Betreiber. Auch die MiFiD II stellt wieder auf den Begriff des »Betriebs« ab[105], so dass auch weder Teilnehmer noch Miner erfasst wären.

100 Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 04. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister. ABL L 201 vom 27. Juli 2012.

101 Diese werden nach Art. 6 Abs. 1 EMIR von der ESMA festgelegt.

102 § 4 BörsG; Art. 44 MiFiD II.

103 § 1 Abs. 1a S. 2 Nr. 1b KWG.

104 Anhang I Abschn. A (8) und (9)

105 BaFin, Merkblatt – Tatbestand des Betreibens eines multilateralen Handelssystems, Stand: 7/2013, S. 2.

6 Auswirkungen auf zentralisierte Banken-Teilbranchen in der Eurozone

6 Auswirkungen auf zentralisierte Banken-Teilbranchen in der Eurozone

Wie bereits eingeführt wurde, hebt der Einsatz von Distributed Ledger Technologien, wie Blockchain oder Ripple, die größten Effizienzpotentiale bei Ökosystemen, die in wesentlichen Elementen zentralistische Wertschöpfungsschritte beinhalten. Dies umfasst sowohl die prozessuale Abfolge als auch die Architektur auf Applikations- und Technologieebene.

Während wir in der, in dieser Ausarbeitung fokussiert betrachteten, Eurozone weder im Einlagen- noch im nicht-syndizierten Finanzierungsgeschäft solche strukturellen Grundzüge wiederfinden, so sind dies doch wesentliche Konstruktionsmerkmale des Wertpapiergeschäfts und des Zahlungsverkehrs unabhängig der zu transferierenden Assets (UTXO[106]). Bei der Betrachtung der Prozesse von der Transaktionsinitiierung über das Clearing bis zum Settlement werden, unter anderem aufgrund regulatorischer und aufsichtsrechtlicher Rahmenbedingungen, hoheitliche Aufgaben zentral wahrgenommen oder zumindest über zentrale Anwendungen bzw. Infrastrukturen abgewickelt. Daher liegt es nahe, die Auswirkungen des Einsatzes möglicher Distributed Ledger Technologien auf die operationalen Modelle im Kapitalmarktgeschäft[107] und im sonstigen Transaction Banking im Sinne möglicher zukünftiger Modelle in einer Einzelbetrachtung aufzuzeigen.

Im Folgenden werden 3 mögliche Modelle im Aufsichtsraum der Eurozone betrachtet, die je nach Anwendungsfall zukünftig auch durchaus in Koexistenz denkbar sind.

106 Unspent Transaction Output – siehe auch Bitcoin developer Guide.

107 Fokus in diesem Dokument ist das Direktanlagegeschäft; spezielle Anforderungen für Investmentfondsgeschäfte aus UCITS und AIFMD werden nicht betrachtet.

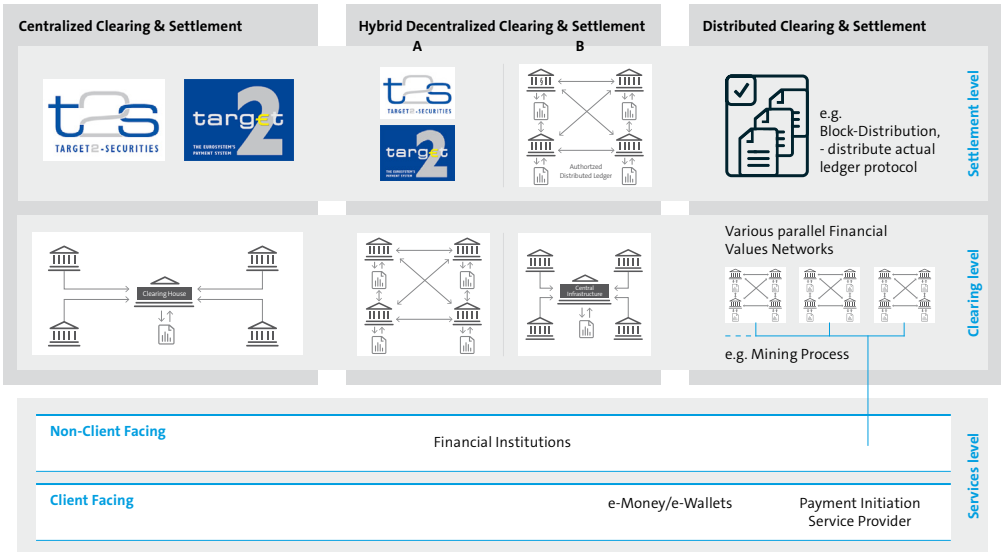


Abbildung 10: Modelloptionen im Zahlungsverkehr und Wertpapiergeschäft

Je nach Einsatzgebiet von DLT-Technologie entlang der Bereiche Services,[108] Clearing (Feststellen gegenseitiger Forderungen, Verbindlichkeiten und Lieferverpflichtungen) und Settlement (Lieferungsabwicklung und Verrechnung) unterscheidet man zwischen dem heute marktüblichen zentralistischen Basismodell, einem Hybridmodell, in dem zentralistische Marktstrukturen unter Einsatz der DLT-Technologie beibehalten werden, und einem völlig dezentralen Modell.

6.1 Das zentralistische Basismodell

Das heutige Modell im Wertpapiergeschäft und im Zahlungsverkehr der Eurozone ist geprägt durch zentralistische Strukturen im Clearing und Settlement Level.

Die Clearing-Funktion sowie auch die Settlement-Funktion wird im Wertpapiergeschäft außerhalb des bilateralen Banken-OTC-Geschäfts zumeist durch nationale bzw. supranationale Dienstleister wie z. B. Eurex Clearing und Clearstream Banking Frankfurt bzw. Luxemburg wahrgenommen. Die darüber hinaus im Börsenhandel mit anonymen Orderbüchern (z. B. Eurex, Xetra) bzw. in der Risikomitigation auch im OTC-Geschäft aufsichtsrechtlich geforderte Rolle eines zentralen Kontrahenten wird durch wenige zentrale Unternehmen, wie z. B. Eurex Clearing, übernommen. Diese oligopolistischen Strukturen sind auch im Zahlungsverkehr durch die Bereitstellung der Verrechnungsfunktionen durch Automated Clearing Houses, wie z. B. durch die Deutsche Bundesbank oder die EBA-Clearing, wiederzufinden. Darüber werden zukünftig

108 In dieser Ausführung Fokussierung auf Transaktionsauslösung; Custody Services sowie Bestandskontenführung werden nicht näher betrachtet.

neben den heutigen SCT[109]-Transaktionen auch SCT^{inst}-Transaktionen, sogenannte instant payments – also Massenzahlungsverkehr in nahezu Echtzeit – zu verarbeiten sein. Dies ist auf eine Initiative der EZB zurückzuführen. Damit ist unter anderem der Anschluss zu bereits im europäischen Nicht-Euroraum, wie beispielsweise in UK und Dänemark, vorzufindenden Realtime Payments Clearing-Systemen herzustellen. Durch den vom mit der Umsetzungsdurchführung beauftragten European Payments Council vorgelegten straffen Zeitplan, der eine Einführung bis Ende 2017 vorsieht, ist bis dahin mit der Konzeption einer z. B. Blockchain-basierten Lösung nicht zu rechnen.

Während für die Wertpapierabwicklung bereits in einigen europäischen Ländern, wie den Niederlanden und UK über Blockchain-basierte Settlement-Wege diskutiert wird, ist man in der übrigen Eurozone inmitten der Vereinheitlichung durch die Anbindung an die neue Target 2 – Securities (T2S) – Plattform. Inwiefern die, auch für Drittwährungen offene, Plattform in Zeiten der Einführung DLT-basierter Technologien seine erhoffte europäische Expansion außerhalb der Eurozone erfahren wird, bleibt abzuwarten.

Der T2S-Ursprung, nämlich Target-2, sorgt bekanntlich für das Settlement des Zahlungsverkehrs in EURO. Dieses erfolgt allerdings nicht real-time, was die Unterlegenheit in Bezug auf den, in manchen anderen Staaten geplanten, Einsatz von Blockchain-Abkömmlingen für diese Funktion deutlich macht.

Auf dem Services Level, also dort, wo Transaktionen im Zahlungsverkehr wie auch im Handel ausgelöst werden, sind die Strukturen zwischen der Interaktion mit dem Endkunden und der Interaktion mit den zentralen Clearing Plattformen zu unterscheiden; letztere sind vorwiegend aufsichtlich zugelassenen Banken bzw. Handelsplattformen vorbehalten, während die Kundenschnittstelle bereits heute von dezentralen und zum Teil unregulierten Marktteilnehmern bedient wird. Betrachtet man den Zahlungsverkehr, so werden sogenannte Zahlungsauslösedienstleister aber auch Kontoinformationsdienstleister zukünftig über die bis 2018 in nationales Recht umzusetzende PSD II[110] von der Regulierung erfasst. Die Einbeziehung von banklizensierten Instituten bei der Anbindung an ACH's[111] ist davon unbenommen. Die Entwicklung von DLT-basierten Zahlungsverkehrs-Services ist besonders bei Cross-border-Zahlungen, sogenannten Remittance-Services, weit fortgeschritten.

Die Übertragung dieser Anwendungen auf den nationalen bzw. SEPA-Zahlungsverkehrsraum wird nicht lange auf sich warten lassen. In naher Zukunft ist somit eine parallele Nutzung von Transaktionsinitiierungen über sowohl traditionelle Anwendungen, als auch Blockchain-basierte Anwendungen zu erwarten. Der Einsatz und die Nutzung von DLT-Strukturen wird allerdings im Wesentlichen dadurch determiniert werden, inwiefern damit die Einhaltung von Marktmissbrauchsrichtlinien, Geldwäschebestimmungen oder auch hoheitliche Ziele wie die Terrorismus-

109 Sepa Credit Transfer Protokoll.

110 Richtlinie (EU) 2015/2366 vom 25. November 2015, ABl. EU vom 23.12.2015, L 337/35; vgl. zur Lizenzpflicht der »dritten Zahlungsdienstleister« ausführlich Matthias Terlau, ZBB 2016, 122 ff.

111 Automated Clearing Houses.

bekämpfung, weiterhin sichergestellt werden können. Dies prägt sicherlich die derzeit geführten Analysen in verschiedenen Zentralbanken bzgl. der Einführung einer virtuellen Geldmengensteuerung mittels eigenentwickelter Kryptowährungen, wie dies bereits in China, UK oder auch den Niederlanden diskutiert wird. Die über Giralgeldschaffung incentivierte Mining-Aufgabe wäre auf Basis einer reinen Kryptowährung beschränkt auf die technische Obergrenze der zu Verfügung stehenden virtuellen Geldmenge und würde langfristig zu einer von den Ledger-Teilnehmern zu honorierenden Aufgabe führen.

Im Vergleich dazu ist das Services Level im Wertpapiergeschäft u. a. geprägt durch zentralistische Handels-Infrastrukturplattformen, ECN's[112], alternative Handelssysteme und Online-Broker. Die Entwicklung DLT-basierter Handelsplattformen ist heute noch auf Einzelproduktebene bzw. verschiedene Handelsbereiche, wie z. B. den Nachhandel komplexer Konstrukte oder der Emission von Unternehmensanleihen, fokussiert. Die Anwendungsbereiche werden sich aber in naher Zukunft sehr schnell ausbreiten. Darüber hinaus sind die DLT-Einsatzbereiche an der Kundenschnittstelle auch bei Peripherie-Themen, wie der Corporate Actions Verarbeitung[113], der Stimmrechtsabgabe bei Aktionärsversammlungen oder auch zur regulatorisch getriebenen Bereitstellung von Informationen eines Transaktionsregisters zu sehen. Insbesondere im Wertpapiergeschäft werden Themen wie Know Your Customer, Datenschutz oder Embargo-Listen-Checks bei der Nutzung von auf Anonymität basierten Interaktionssystemen zu erfüllen sein. Die Anwendungsbereiche sind somit sehr vielfältig.

Mit Blick auf die eingangs erwähnte – zumindest kurz- bis mittelfristig – erwartete Koexistenz der Strukturmodelle wird das zentralistische Basismodell, insbesondere durch seine politische Akzeptanz auf dem Clearing- und Settlement Level, auch weiterhin in der Eurozone maßgeblich prägend sein. Die meisten und kurzzeitig zu erwartenden Änderungen bzw. Ergänzungen werden im Services Level im Rahmen spezieller Teildienstleistungen oder Produktbereiche bzw. Zahlungsarten vorzufinden sein. Die Interoperabilität von DLT-basierten Architekturen und der bestehenden Wertpapier- bzw. Zahlungsverkehrsarchitekturlandschaft wird dabei wesentlicher, erfolgskritischer Faktor sein.

Darüber hinaus werden die regulatorischen Rahmenbedingungen die Etablierung der Technologie am Markt entscheidend beeinflussen. Im Gegensatz zur konservativen Haltung der BaFin hat die britische Aufsichtsbehörde (Financial Conduct Authority = FCA)[114] bereits die Zulassungsbereitschaft von DLT-Diensten innerhalb ihrer Sandboxing-Unterstützung von FinTechs signalisiert.

112 Electronic communication network.

113 Weitergehende Ausführungen über die Zukunft bzw. den Wegfall von Custody-Funktionen sind nicht Bestandteil dieses Dokuments.

114 ↗ https://news.bitcoin.com/fca-considers-blockchain-approval

6.2 Das Hybridmodell

In der Kombination der Vorteile von dezentralen und zentralen Elementen im Wertpapiergeschäft und Zahlungsverkehr ist eine hybride Modellstruktur – insbesondere in Bezug auf Clearing und Settlement – ein realistisches Szenario. Die Aspekte des Services Levels beim Auslösen einer Transaktion oder eines Handelsgeschäfts wären dabei analog zum zuvor dargestellten Basismodell.

In einer ersten Variante würden die im Basismodell dargestellten Clearing-Infrastrukturen zum Einsatz kommen. Kombiniert würde dies allerdings mit einer DLT-basierten Settlement Struktur, wie sie heute bereits in UK beispielhaft für den Zahlungsverkehr angedacht wird. Dies hätte zur Folge, dass sowohl auf Clearing als auch auf Settlement Level eine real-time Verarbeitung ermöglicht würde.

In diesem Settlement-Modell würden sich Aufsichtsbehörden oder Zentralbanken als ein »Node« des Distributed Ledger Netzwerks integrieren und würden damit über eine real-time Einsicht in die getätigten Geschäfte verfügen. Ein umfängliches Reporting – z. B. für SFTR,[115] MAR[116] und AMLD[117] – würde deshalb hinfällig, denn die Daten könnten direkt in das sich im Aufbau befindende European Reporting Framework einfließen. Voraussetzung dafür wäre, dass der Algorithmus der genutzten Distributed Ledger Technologie von hoheitlicher Stelle entwickelt würde bzw. allgemein anerkannter und akzeptierter Open Source ist; d. h. beispielsweise die EZB oder ein qualifizierter Zentralverwahrer eines Landes würde eine eigene öffentliche Blockchain zur Abwicklung einzelner Wertpapiergeschäfte oder Zahlungsverkehrstransaktionen bereitstellen. Das Distributed Ledger-Netzwerk müsste dabei in einer gesicherten public cloud Infrastruktur bereitgestellt werden; aufsichtliche Compliance insbesondere bzgl. CSDR[118] und SFD[119] wären zu beachten; die Zulassung von Netzwerkteilnehmern würde das ESZB oder die jeweils zuständige NCA[120] übernehmen, die jeweils nationale Wallets bereitstellen würde. Zu klären wäre die Einführung eines EURO-Coin für das Mining oder eine auch derzeit untersuchte Kryptowährungs-unabhängige Konsensfindungsmethode, analog zum heutigen Bitcoin-Mining.

Private DLT-basierte Lösungen im dezentralen Umfeld, wie sie teilweise heute schon bei der Emission und dem Handel von Unternehmensanleihen vorzufinden sind, wären davon unabhängig.

Eine alternative Hybridvariante ist die Verknüpfung von DLT-basierter Transaktionsinitiierung und Clearing mit zentralem Settlement über T2S im Wertpapiergeschäft bzw. Target-2 im Zahlungsverkehr. Im Hinblick auf die politische Verständigungsnotwendigkeit in der Eurozone bzgl.

115 Securities Financing Transaction Regulation.

116 Market Abuse Regulation.

117 Anti-Money Laundering Directive.

118 Central Securities Repositories Regulation.

119 Settlement Finality Directive.

120 National Competent Authority.

hybrider Lösungen, erscheint diese Option als realistischer, da damit auch die Investitionen in Target-2 und T2S gerechtfertigt erscheinen. Allerdings sind die aufsichtsrechtlichen Vorschriften insbesondere aus EMIR und MIFIR bzgl. der Aufgaben des CCP's für OTC-Derivate-bzw. ETD-Clearing, Risk Management, Margining und Collateral Management zu berücksichtigen, die potentielle DLT-Effizienzpotentiale limitieren.

6.3 Das dezentrale Modell

Bei der vollständigen Nutzung von DLT-basierten Abläufen werden im Wertpapiergeschäft die Handels-, Clearing- und Settlement – Funktionen komplett zusammenfallen. Dies beinhaltet eine dezentrale Trade-Initiation mit dem jeweiligen Counterpart, die ein sofortiges Clearing und Settlement nach sich zieht. Netting von Positionen ist innerhalb desselben Blocks mit demselben Hashwert und zwischen den gleichen Kontrahenten denkbar. Limitiert wird dies bei der Verwendung der Blockchain-Technologie durch die Mining-Zeit zur Überprüfung eines neuen Blocks. Die Funktion des, für die vorgenannten Marktsegmente und Börsenformen bisher aufsichtlich geforderten, zentralen Kontrahenten würde obsolet werden, da ein Kontrahentenausfallrisiko durch das Zusammenführen von Verpflichtungs- und Erfüllungsgeschäft in einem einzelnen Block nicht mehr bestehen würde. Die bislang durch den zentralen Kontrahenten durchgeführten Risikomitigationen durch Margin Calls könnten ebenso über Smart Contract – Konstruktionen abgebildet werden. Auch die zentralen Handels-, Clearing- und Settlement-Stellen werden dadurch überflüssig werden; die erforderliche transparente Preisfeststellung wird über die permanente Verteilung des Distributed Ledgers zu gewährleisten sein. Die Aufsicht kann wie im zuvor beschriebenen Hybridmodell als »Node« am Netzwerk informativ teilnehmen und so als Kontroll-, Aufsichts- sowie Reporting-Organ partizipieren. Wie bereits in 2.2 aufgezeigt müssen aber auch hier die aufsichtsrechtlichen Funktionszuordnungen des CCPs, wie in EMIR und MIFIR festgelegt, Berücksichtigung finden.

Die Funktionen eines Market Makers könnten unter anderem über Smart Contracts protokolliert werden. Damit könnte eine Gegentransaktion des Market Makers zur Glattstellung von Positionen und Liquiditätssteuerung zu gegebenem späteren Zeitpunkt stattfinden; die Minimierung seiner Risikopositionen – auch durch den Einsatz von Instrumenten mit anderen zugrundeliegenden Basiswerten wie z. B. durch Index-Futures – kann davon unabhängig stattfinden. Dem Regulator muss durch entsprechende Information, beispielsweise über den encryption Key des Market Makers verschlüsselt, Einblick über dessen Aktivitäten gewährt werden. Es sind hierbei zwei Funktionen des Market Makers und der damit über das Distributed Ledger Netzwerk verteilten Informationen zu unterscheiden. Einerseits werden die durch ihn getätigten Geschäfte in dem durch ihn verantworteten Instrument – unabhängig ob Ausgleichsgeschäfte eigener Positionen oder klassische Vermittlungsgeschäfte zwischen den Marktteilnehmern,– in der Form von Einzeltransaktionen verteilt. Andererseits kann er der Pre-Trade Transparenz entsprechend seiner Quotierungsverpflichtung dadurch nachkommen, in dem z. B. ein sogenannter Coloured Token als Informationsträger verwendet wird, um die aktuellen Quotes und Spreads für den Markt zu visibilisieren. Dies bedeutet, dass die für die eigentliche Kryptowährung vorgesehene Stelle des

Protokolls mit der Information einer Quotierung überschrieben wird, um lediglich die Information über aktuelle Spreads im Markt zu verteilen, ohne einen Trade zu tätigen. Jedoch ist unter Berücksichtigung der aktuell verfügbaren Mining-Prozess-Kapazitäten bei der Nutzung einer Blockchain und der dadurch entstehende Mindestberechnungszeiten eines neuen Blocks die heutige automatische hochfrequente Quotes-Veröffentlichung – wie sie über sogenannte Quote-Roboter durchgeführt wird – schwer abbildbar.

Die Distribution des Wallet-Zugangs, die Entwicklung des DLT-Algorithmus sowie des DLT-Netzwerks, z. B. via Cloud, und – abhängig von der eingesetzten Technologie – die entsprechenden Mining-Funktionen werden beim offenen Handel in einer public-Variante optimaler Weise ganzheitlich von einem DLT-Engineering Unternehmen bereitgestellt. Analog ist beim geschlossenen Handel, z. B. bei der Neu-Emission von Wertpapieren im primary market, eben in einer private-Variante zu verfahren. Die Bereitstellung der notwendigen Funktionen ist allerdings auch arbeitsteilig durch mehrere Dienstleister denkbar. Eine derzeit durchaus einschlägige Kombination ist die Bereitstellung einer Cloud-Infrastruktur eines Unternehmens, auf der dann der Open Source DLT-Algorithmus eines anderen Dienstleisters betrieben wird.

Analog ist dies auch im Zahlungsverkehr abbildbar. Dies würde allerdings die derzeit konzipierten Instant Payments Systemweiterentwicklungen bewährter Anbieter sowie Target-2 überflüssig machen. Die parallele Abwicklung unterschiedlichster Zahlungsformate ist durch die Protokollierung über Smart Contracts darstellbar, um so den Zeitverzug insbesondere bei Kartenzahlungen zu implementieren.

Stellt man die vorgestellten Modelle gegenüber, so wird deutlich, dass je nach Anwendungsbereich jede Struktur seine Zukunftsfähigkeit hat. Wesentlich entscheidend für die Fortschreibung zentralistischer Modelle oder Modellbestandteile wird die Entwicklung aufsichtlicher bzw. politischer Entscheidungsprozesse sein. Die dafür notwendigen regulatorischen Veränderungen wären nicht unerheblich.[121] Die den Marktteilnehmern in Aussicht gestellten Kosteneinsparungen werden realisiert werden können, wenn auch die Interoperabilität zwischen mehreren DLT-basierten Strukturen und Schnittstellen zu restlichen Unternehmensarchitekturen sowie zentralen Elementen sichergestellt werden können.

121 Vgl. auch oben Kapitel 5.3.

7 Fazit und Ausblick

7 Fazit

Es ist sicherlich verfrüht sich zu einer Bewertung hinsichtlich des disruptiven Potentials der eben erst begonnenen Forschung und Entwicklung von Distributed Ledger Technologien wie der auf spieltheoretischen Ansätzen basierenden Blockchain hinreißen zu lassen. Im Vergleich zur Verbreitung von TCP/IP bis hin zum Internet, mit der diese technologische Innovation des Öfteren verglichen wird, befinden wir uns Mitte der 90er Jahre. Dabei ist aber bereits jetzt unbestritten, dass wir nach den Mainframe- und Client Server Architekturen durch diese Technologie einen weiteren zumindest evolutionären Meilenstein in Richtung »Decentralized Computing Technologies« erleben. Durch die Eliminierung der Notwendigkeit zentraler Serverstrukturen ergeben sich analoge Rechtsfragen, wie bei der Entwicklung des Internets in Bezug auf unterschiedliche Rechtsräume. Eine kurz- bis mittelfristige Konvergenz wäre zwar mehr als angebracht, nüchtern betrachtet aber politisch utopisch.

Welche der Distributed Ledger Technologien ihre reale Verbreitung finden wird, ist noch nicht abzusehen; ob die ursprüngliche Bitcoin-Blockchain zukünftig eher eine untergeordnete Rolle im Vergleich zu Ablegern, wie der Ethereum-Blockchain oder doch davon unabhängige Entwicklungen wie Ripple oder Corda überwiegen werden, ist aus der Sicht der ursprünglich verfolgten demokratischen – zuweilen auch als anarchistisch bezeichneten – Grundprinzipien von nachrangiger Bedeutung. Das Ziel verteilte Datenstrukturen und Transaktionsprotokolle transparent, nachvollziehbar, anonymisiert und in ihrer Finalität unveränderlich sowie konsensual ermittelt bereitzustellen, findet mittlerweile nicht mehr bei allen Weiterentwicklungen Berücksichtigung.

Die Anwendungsgebiete sind vielfältig. Sie reichen von Zahlungsverkehrsanwendungen, Smart Contracts bei Handelsfinanzierungs-Prototypen bis zur Abdeckung unterschiedlichster Wertschöpfungsbestandteile im Wertpapierhandel. Insbesondere bei zuletzt genannter Banking-Teilbranche werden die höchsten Effizienzgewinne erwartet; allerdings ist dabei zu berücksichtigen, dass die bestehenden regulatorischen Rahmenbedingungen in wesentlichen Bereichen nur zentrale Kontrahenten oder Zentralverwahrer als DLT-Betreiber zulassen würden. Für eine größere Öffnung des Marktes müssten wesentliche aufsichtsrechtliche Rahmenbedingungen der letzten 10-15 Jahre angepasst werden, was aufgrund der europäischen Gesetzgebungsverfahrensdauern auf keine kurzfristigen Veränderungen schließen lässt.

Im Hinblick auf die Transformation heutiger Geschäftsarchitekturen werden sowohl DLT-Netzwerk-übergreifende als auch hybride Strukturen zwischen aktuellen Bestandssystemen und deren Anbindung an öffentliche und private bzw. konsortiale Netzwerke zu erwarten sein. Je nach Ausprägung ist dabei auch eine Einbindung aufsichtlicher Stellen als ›Node‹ zu erwarten. Inwiefern dabei auch die Möglichkeit der Hebung von Effizienzgewinnen in Bezug auf den Wegfall gesonderter Meldewesenschnittstellen realisiert werden wird, bleibt abzuwarten. Mit großem Interesse wird auch die Entwicklung der viel Potential zugesprochenen Grundidee der DAOs[122] zu verfolgen sein. Inwiefern sich die auf Smart Contracts beruhenden autonomen Netzwerke auch in der Finanzindustrie durchsetzen werden, bleibt abzuwarten.

122 Decentralized Autonomous Organizations.

Diese Entwicklung wird im Wesentlichen dadurch geprägt werden, welche Zielsetzungen die beteiligten Netzwerkpartner beim Einsatz von Distributed Ledger Technologien wie der Blockchain verfolgen werden. Neben der Optimierung bestehender Geschäftsmodelle durch Kosteneinsparungen, verbesserter Liquiditätssteuerung und Schnelligkeit sind auch der Erhalt bzw. die Ermöglichung neuer Geschäftsmodelle nachvollziehbare Zielsetzungen. Andererseits sind durchaus auch Beweggründe in Bezug auf die Anonymität von DLT-Strukturen von Bedeutung, wenn man die Thematiken Briefkastenfirmen, Geldwäsche oder Finanzierung von kriminellen Handlungen in Betracht zieht.

Diese Themen werden sicher nicht autark in der Finanzdienstleistungsindustrie fortgeschrieben werden, sondern durch die enge Vernetzung mit banknahen Industrien wie beispielsweise dem Handel und der Telekommunikationsindustrie weiter entwickelt werden. Darüber hinaus ist der gegenseitige Einfluss anderweitiger technologischer Entwicklungen wie z. B. des ›Internet of Things‹ in Verbindung mit Distributed Ledger Technologien von übergeordneter Bedeutung, was heutige Anwendungsbeispiele bereits aufzeigen.

Der politische Diskurs zwischen dem technisch Machbaren der Technologie und dem gesellschaftlich wie ökonomisch Gewollten hat noch nicht richtig begonnen, da bereits heute nicht jeder DLT-Anwendungsfall zwingend den Einsatz eines Blockchain-Netzwerks erfordert. Viele Intermediärfunktionen, die in der Vergangenheit erfolgreich etabliert wurden, wären technologisch obsolet.

Aufgrund der immer kürzer werdenden Halbwertszeiten der DLT-Innovationen gilt es die Herausforderung als Chance zu verstehen, mit Augenmaß abzuwägen, inwieweit diese mikro- bzw. makroökonomischen Funktionen auch unter Nutzung der neuen Technologie abzubilden wären und den dafür notwendigen flexiblen Rechtsrahmen zu schaffen.

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 79 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, weitere 9 Prozent kommen aus Europa, 8 Prozent aus den USA. 4 Prozent stammen aus Asien, davon die meisten aus Japan. Bitkom fördert die digitale Transformation der deutschen Wirtschaft und setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom