Risiken und Chancen von Kryptowährungen

Technik, rechtliche Grundlagen, wirtschaftliche Potenziale

Masterthesis

Fakultät Wirtschaft und Soziales - Department Wirtschaft
Studiengang International Logistics and Management
an der
Hochschule für Angewandte Wissenschaften Hamburg

Hochschule für Angewandte
Wissenschaften Hamburg
Hamburg University of Applied Sciences

vorgelegt von:

Jan Rusche [redacted]

Betreuender Professor: Herr Prof. Dr. Josef Kovač
Zweiter Prüfender: Herr Dipl.-Kfm. Holger Kopietz

Abgabedatum: 20.12.2018

Inhaltsverzeichnis

Inhaltsverzeichnis I

Abbildungsverzeichnis III

Tabellenverzeichnis IV

Abkürzungsverzeichnis V

1 Einleitung 1

1.1 Ausgangssituation 1

1.2 Zielsetzung 2

1.3 Methodisches Vorgehen 3

1.4 Kritische Würdigung der Literatur 4

2 Grundlagen des Geldes und aktuelle Zahlungsmethoden 6

2.1 Geschichte und Funktionen des Geldes 6

2.2 Aktuelle Zahlungsmethoden 9

2.3 Zahlungsverkehr im digitalen Wandel 12

3 Die Blockchain-Technologie 17

3.1 Funktionsweise der Blockchain 19

3.2 Konsens-Algorithmen 24

3.3 Die unterschiedlichen Arten der Blockchain 26

3.4 Kryptografie 29

3.5 Mining 32

4 Kryptowährungen 36

4.1 Bitcoin (BTC) 36

4.2 Alternative Kryptowährungen (Altcoins) 38

4.2.1 Ether (ETH) 38

4.2.2 Ripple (XRP) 41

4.2.3 IOTA 44

4.3 Handel und Aufbewahrung von Kryptowährungen 47

4.4 Initial Coin Offering (ICO) 50

5 Rechtliche Grundlagen 54

5.1 Datenschutzrecht 54

5.2 Zivilrecht 57

5.3 Steuerrecht 62

5.4 Lizenzrecht 67

5.5 Ländervergleich aus rechtlicher Perspektive 69

6 Risiken von Kryptowährungen und Blockchain 73

6.1 Akzeptanz und Komplexität 73

6.2 Skalierbarkeit 76

6.3 Ressourcenverbrauch 80

6.4 Volatilität 83

6.5 Fehlende zentrale Instanz und rechtliche Unsicherheiten 85

6.6 Sicherheit 87

7 Chancen von Kryptowährungen und Blockchain 90

7.1 Kostensenkung und Effizienzsteigerung 90

7.2 Dezentralität 91

7.3 Transparenz und Anonymität 94

7.4 Vorreiterrolle 96

7.5 Anwendungsspezifische Chancen und Potenziale 97

7.5.1 Beispiel Supply Chain Management 99

7.5.2 Beispiel Finanzbranche 103

7.5.3 Beispiel Energiewirtschaft 105

7.5.4 Beispiel öffentlicher Sektor 107

8 Mögliche Entwicklungsszenarien 111

9 Zusammenfassende Schlussbetrachtung 114

Literaturverzeichnis VIII

Abbildungsverzeichnis

Abb. 1: Kursverlauf Bitcoin vom 01. Jan. 2017 bis 13. Aug. 2018 15

Abb. 2: Vereinfachtes Schema einer Blockchain 18

Abb. 3: Bitcoin-Transaktion 20

Abb. 4: Bestandteile eines Blocks 23

Abb. 5: Kursverlauf Ether vom 01. Jan. 2017 bis 13. Aug. 2018 40

Abb. 6: Kursverlauf Ripple vom 01. Jan. 2017 bis 17. Okt. 2018 43

Abb. 7: Kursverlauf IOTA-Token vom 13. Jun. 2017 bis 21. Okt. 2018 45

Abb. 8: Tangle-Struktur von IOTA 46

Abb. 9: Höhe der ICO-Investitionen 52

Abb. 10: Beispiel für eine blockchainbasierte Supply Chain 100

Tabellenverzeichnis

Tab. 1: SHA256-Ausgabewerte..... 30

Tab. 2: Erwartete Entwicklungstendenzen der Einflussfaktoren..... 111

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
Altcoins	Alternative Coins
Anlage SO	Sonstige Einkünfte
App	Applikation
ASIC	Application Specific Integrated Circuit
B2B	Business to Business
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BCH	Bitcoin Cash
BGB	Bürgerliches Gesetzbuch
BTC	Bitcoin
CBDC	Central Bank Digital Currencies
CFD	Contracts For Difference
CFTC	Commodity Futures Trading Commission
CO2	Kohlenstoffdioxid
CPU	Central Processing Unit
DAO	Dezentralisierte Autonome Organisation
dApp	Dezentralisierte Applikation
DNS	Desoxyribonukleinsäure
DSVGO	Datenschutzgrundverordnung
E-Commerce	Elektronischer Handel
E-Geld	Elektronisches Geld
E-Payment	Elektronische Bezahlung
E-Person	Elektronische Person
E-Voting	Elektronische Wahlen
E-Wallet	Elektronische Geldbörse

EStG	Einkommenssteuergesetz
ETH	Ether
EU	Europäische Union
EZB	Europäische Zentralbank
FIFO	First In First Out
GewStG	Gewerbesteuergesetz
GmbH	Gesellschaft mit beschränkter Haftung
GH/s	Gigahashes pro Sekunde
GPU	Graphics Processing Unit
H/s	Hashes pro Sekunde
I-Voting	Internetwahlen
IBAN	International Bank Account Number
IBM	International Business Machines Corporation
ICO	Initial Coin Offering
IPO	Initial Public Offering
IoT	Internet of Things
IOTA	Internet of Things Application
IOU	I owe you
KfW	Kreditanstalt für Wiederaufbau
KWG	Kreditwesengesetz
LSE	London School of Economics
LTC	Litecoin
M2M	Machine to Machine
MIOTA	Eine Million IOTA
NASDAQ	National Association of Securities Dealers Automated Quotations

P2P	Peer-to-Peer
PIN	Persönliche Identifikationsnummer
PoW	Proof-of-Work
PoS	Proof-of-Stake
PoI	Proof-of-Importance
PwC	PricewaterhouseCoopers International
QR-Code	Quick Response Code
SHA	Secure Hash Algorithm
SPV	Simplified Payment Verification
STO	Security Token Offering
UStG	Umsatzsteuergesetz
XRP	Ripple
ZAG	Zahlungsdiensteaufsichtsgesetz

Abstract

Die vorliegende Masterthesis beschäftigt sich mit Chancen und Risiken von Kryptowährungen und der Blockchain-Technologie. Dazu werden Fragen formuliert, ob sich aus unternehmerischer Sicht realistische Anwendungschancen ableiten lassen und welche Risiken sich aus der Entwicklung der letzten Jahre ergeben. Aufbauend auf einer detaillierten Darstellung der technischen und rechtlichen Grundlagen werden durch zahlreiche Fachartikel, vorhandene Studien und Fachliteratur, Potenziale in vielen Anwendungsbereichen identifiziert. Doch dem stehen aufgrund rechtlicher Unsicherheiten, Akzeptanzproblemen und technischer Limitationen zahlreiche Risiken gegenüber, die es abzuwägen gilt. Vieles ist derzeit noch ungewiss, jedoch werden nach mehrheitlicher Meinung die Vorteile auf Dauer überwiegen und Kryptowährungen Einzug in den Alltag finden. Daraus lässt sich ableiten, dass Unternehmen sich dieser Herausforderung stellen und die Thematik in ihre Unternehmensstrategie aufnehmen sollten. Dabei gilt es zu beachten, dass für eine erfolgreiche Implementierung eine individuelle Betrachtung der einzelnen Unternehmen und deren Charakteristika erfolgen muss.

Diese Masterthesis richtet sich insbesondere an Personen oder Unternehmen, die erstes theoretisches Grundwissen zu Kryptowährungen erwerben und sich einen Überblick über die Chancen, Risiken und Potenziale verschaffen wollen. Zudem soll diese Arbeit als Grundlage weiterer Forschungsfragen dienen, die sich beispielsweise retrospektiv mit einer Analyse realisierter Potenziale in unterschiedlichen Branchen beschäftigen.

1 Einleitung

1.1 Ausgangssituation

Der fortschreitende digitale Wandel und das Internet der Dinge (Internet of Things – IoT) haben in den letzten Jahren verschiedene Bereiche der Wirtschaft stark beeinflusst. Neben vielen Innovationen gab im Jahr 2009 eine weitere wegweisende Innovation im Bereich der Zahlungsmethoden – die Einführung von Kryptowährungen. Zuvor nur einigen IT-Insidern bekannt, stieg der Bekanntheitsgrad mit der Einführung des Bitcoins im Jahr 2009 rasant an. Die dahinterliegende Blockchain-Technologie wird als Revolution betrachtet und viele Experten sagen ihr eine goldene Zukunft voraus.[1]

Durch die steigende Anzahl verschiedener Kryptowährungen und der stetigen medialen Präsenz sind auch Unternehmen auf diese Technologie aufmerksam geworden. Ausgehend von einigen Start-Ups, die sich beispielsweise der Zahlung per Bitcoin verschrieben haben, entdecken auch zunehmend namhafte Unternehmen diese Technologie für sich. Darunter ist beispielsweise Samsung, die aktuell die Implementierung einer Blockchain in ihre Supply Chain prüfen.[2] Sogar Staaten, wie beispielsweise Russland oder der Iran, prüfen Einsatzmöglichkeiten für Kryptowährungen. In Venezuela gibt es bereits seit einiger Zeit die staatliche Kryptowährung Petro, die die gesetzten Hoffnungen allerdings noch nicht erfüllen kann.[3]

Die Chancen und Risiken, aber auch der disruptive Charakter der Kryptowährungen und Blockchain-Technologie macht es für Unternehmen mit Blick auf die Zukunft notwendig, sich dieser Herausforderung zu stellen. Aktuelle Geschäftsmodelle könnten sich grundlegend verändern – analysieren Unternehmen die sich ergebenen Chancen und Risiken nicht rechtzeitig, besteht die Gefahr, von der Konkurrenz abgehängt zu werden. Zudem bestehen Chancen für die Entstehung vollkommen neuer Geschäftsfelder. Es ist also unerlässlich, ein Verständnis dafür zu entwickeln und sich mit aktuellen Entwicklungen zu beschäftigen.

---

1 Vgl. Specht (2018), S. 219.

2 Vgl. Wired (2018) (abgerufen am 02. Sept. 2018).

3 Vgl. Mühlbauer (2018) (abgerufen am 02. Sept. 2018).

Dabei begehen viele anfänglich direkt einen Fehler. Die Blockchain-Technologie ist so viel mehr als nur Bitcoin und es gibt inzwischen zahlreiche, weitaus ausgereiftere und effizientere Alternativen (auch als Altcoins oder alternative Coins bezeichnet), wie beispielsweise Ether oder IOTA (Internet of Things Alliance). Viele dieser Altcoins bieten für Unternehmen interessante Ansätze zur praktischen Implementierung in bestehende Geschäftsprozesse.

Aber auch losgelöst von Kryptowährungen bietet die Blockchain-Technologie ein gewaltiges Potenzial. Aktuell bekommt dieses Thema allerdings eher durch enorme Spekulationsgewinne und -verluste der einzelnen Kryptowährungen eine mediale Präsenz. Zwar rücken zuletzt auch häufiger die mit der Blockchain verbundenen wirtschaftlichen Chancen in den Fokus – oft wird das gesamte Thema jedoch als riesige Spekulationsblase betrachtet, die in einigen Jahren wieder verschwunden ist.[4] Zudem konnte sich bisher keine Kryptowährung für den alltäglichen Zahlungsgebrauch durchsetzen, obwohl die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bereits im Jahr 2013 virtuelle Währungen als Recheneinheit und möglichen Bargeldersatz anerkannt hat.[5] Vielen Unternehmen, die bereits in der Vergangenheit nicht sehr aufgeschlossen gegenüber Innovationen waren, droht durch die negative Berichterstattung, dass sie von dieser Entwicklung abgehängt werden. Es liegt dabei auch am Unternehmen und der Philosophie selbst, wie offen technischen Neuerungen entgegengetreten wird.

Eben diese Skepsis, aber auch der disruptive Charakter schaffen eine Notwendigkeit, Unternehmen die technischen und rechtlichen Grundlagen sowie Potenzial, aber auch Risiken, aufzuzeigen. Zudem befindet sich die gesamte Thematik noch sehr am Anfang, weshalb Literatur sowie aktuelle Studien nur im geringen Maße verfügbar sind.

1.2 Zielsetzung

Die Zielsetzung dieser Masterthesis ist es, die wirtschaftlichen und gesellschaftlichen Chancen und Risiken von Kryptowährungen zu identifizieren. Dazu sollen insbesondere der technische Aspekt und die rechtlichen Grundlagen analysiert und verständlich wiedergegeben werden. Es soll ein Bewusstsein geschaffen werden, dass weder Blockchain = Kryptowährung, noch Blockchain = Blockchain ist. Seit der Entstehung

[4] Vgl. Specht (2018), S. 219.

[5] Vgl. Rosenberger (2018), S. 3.

der Bitcoin-Blockchain sind fast zehn Jahre vergangen und auch in diesem Bereich gibt es Entwicklungen, die starke Innovationen hervorbringen. Darüber hinaus sollen mögliche Anwendungsfelder aufgezeigt werden, in denen Kryptowährungen und Blockchain ihr Potenzial entfalten können. Dies soll auch gleichzeitig als Ausgangspunkt weiterer Forschungsansätze dienen.

Ziel ist es zudem, eine derzeitige Einschätzung der Entwicklungsmöglichkeiten abzugeben und abschließend mögliche Szenarien aufzuzeigen, in die sich Kryptowährungen entwickeln könnten. Im Rahmen dieser Masterthesis finden weder Experteninterviews noch eigene empirische Studien Anwendung – daher gilt es, mit vorhandenen Daten ein realistisches Bild über derzeitige Chancen und Risiken zu schaffen.

Folgende zentrale Fragen sollen im Laufe der vorliegenden Arbeit geklärt werden:

- Bestehen abseits vom Hype für Unternehmen realistische Chancen und Anwendungspotenziale?
- Welchen Risiken stehen Unternehmen durch die derzeitige Entwicklung der Kryptowährungen und Blockchain gegenüber?

Der Fokus liegt dabei auf dem wirtschaftlichen Kontext und nicht, wie derzeit oft in den Medien diskutiert, auf Kryptowährungen als reines Spekulationsobjekt.

1.3 Methodisches Vorgehen

In Kapitel 2 werden, ausgehend vom einleitenden Kapitel 1, zunächst die Grundlagen des Geldbegriffes erläutert. Dazu werden kurz die Geschichte und die Funktionen des Geldes im Kontext des Vertrauensbegriffes dargestellt. Anschließend erfolgt eine Übersicht über derzeitige Zahlungsmethoden, die in Teilen bereits durch die Digitalisierung beeinflusst worden sind und zunehmend in Frage gestellt werden. Abschließend wird detailliert auf den digitalen Wandel im Zahlungsverkehr eingegangen, der gleichzeitig auch den Übergang zu Kapitel 3 darstellt.

Dort wird die Blockchain-Technologie ausführlich dargestellt und anhand eines simplen Transaktionsbeispiels mit der Kryptowährung Bitcoin erklärt. Zudem erfolgt eine Übersicht über weitere Mechanismen zur Konsensfindung, die für eine zukünftige Anwendung womöglich bessere Alternativen darstellen. Darüber hinaus wird das kryptografische Verfahren des vorher beschriebenen Transaktionsbeispiels näher erläutert,

um die Sicherheit der Blockchain-Technologie zu verdeutlichen. Abgerundet wird der technische Abschnitt durch die Darstellung des Minings im Bitcoin-Netzwerk.

In Kapitel 4 folgen, aufbauend auf den Grundlagen der Blockchain-Technologie, die Kryptowährungen. Ausgehend von der Geschichte der Entstehung des Bitcoins spielen auch die Altcoins eine zentrale Rolle in Hinblick auf eine zukünftige Anwendung im Alltag. Darauf folgen eine Übersicht über die sogenannten Wallets, in denen Kryptowährungen verwahrt werden, sowie eine Erklärung des grundsätzlichen Handels mit Kryptowährungen. Eine Form der Interaktion von Unternehmen (insbesondere Start-Ups) mit Kryptowährungen ist das Initial Coin Offering (ICO), welches das Kapitel über die Kryptowährungen abschließt.

In Kapitel 5 werden die rechtlichen Grundlagen behandelt, die in Verbindung mit Kryptowährungen eine Rolle spielen. Dazu zählen Datenschutzrecht, Zivilrecht, Steuerrecht und Lizenzrecht. Abgeschlossen wird dieses Kapitel durch einen Ländervergleich aus rechtlicher Perspektive.

Ausgehend von vorherigen Kapiteln, folgt in Kapitel 6 eine detaillierte Übersicht über die derzeitigen Risiken, die in Verbindung mit Kryptowährungen stehen. Dem gegenübergestellt werden in Kapitel 7 die möglichen Chancen. Um diese Chancen für die wirtschaftliche Anwendung zu verdeutlichen, wird dieses Kapitel durch eine Darstellung praktischer Beispiele in diversen Branchen abgeschlossen.

Im vorletzten Kapitel 8 werden als Ausblick mögliche Entwicklungsszenarien skizziert.

Die gewonnen Erkenntnisse werden abschließend in Kapitel 9 zusammengefasst und mit einem kurzen Ausblick abgeschlossen.

1.4 Kritische Würdigung der Literatur

Das Forschungsthema dieser Masterthesis ist sehr aktuell. Wie bereits angemerkt, ist Literatur dazu nur in einem begrenzten Maße verfügbar. Dadurch ist es wichtig, alternative Quellen heranzuziehen. Viele große Nachrichtenmedien berichten regelmäßig über das Thema, darunter das Handelsblatt, die Sueddeutsche Zeitung oder die Frankfurter Allgemeine Zeitung. Insbesondere wenn es um aktuelle Zahlen oder Entwicklungen geht, wird auf diese Quellen verwiesen, da Zahlen aus Literaturquellen von 2017 oder Anfang 2018 teilweise veraltet sind und sich Daten inzwischen geändert haben.

Zusätzlich werden viele Blogs oder Kryptomagazine als Informationsquellen verwendet, da die dortigen Experten das sehr komplexe Wissen oft verständlich und punktgenau vermitteln. Beispiele dafür sind unter anderem das BTC-Echo oder Crypto Magazin. Viele dieser Magazine publizieren ihre Artikel ausschließlich im Internet.

Die Häufigkeit der Verwendung dieser Quellen ist zwar unüblich für eine wissenschaftliche Arbeit, verspricht aber durch die Aktualität der Zahlen und den vielen Experten den besten Kenntnisgewinn zu dieser Thematik. Sie schaffen unterschiedliche Perspektiven und erklären komplexe, technische Themen mit einfachen Beispielen. Es wird versucht, bei grundlegenden Fakten auf Fachliteratur zu verweisen und diese mit aktuellen Zahlen und Daten aus Onlinemedien anzureichern.

Darüber hinaus wurde im Rahmen der Werkstudententätigkeit bei der Otto GmbH & Co KG in Hamburg ein Vortrag mit dem Titel ‚Blockchain – eine revolutionäre Idee und ihr reelles Potenzial' besucht. Der Referent war der leitende Professor des Fraunhofer Blockchain-Labors, Prof. Dr. Gilbert Fridgen. Neben den technischen Grundlagen lag der Fokus insbesondere auf Fallbeispielen und dem Weg für Unternehmen in die Blockchain-Technologie, welchen das Fraunhofer Institut als Schnittstelle zwischen Forschung und Wirtschaft begleitet. Dadurch wurden viele Erkenntnisse über Chancen, aber auch Hürden von Unternehmen und Organisationen bei der Implementierung von Blockchain und Kryptowährungen als Abwicklungsmedium in ihre Geschäftsprozesse gewonnen.

Die Quellen wurden alle so gewählt, dass sie diese Thesis zu einem bestmöglichen Ergebnis führen sollen.

2 Grundlagen des Geldes und aktuelle Zahlungsmethoden

Kryptowährungen und Blockchain wollen in Konkurrenz zu konventionellen Zahlungsmethoden und -systemen treten oder diese zumindest sinnvoll ergänzen. Aus diesem Grund soll zunächst ein Überblick über die Geschichte des Geldes und dessen Funktionen geschaffen werden. Anschließend rückt der Fokus auf die Zahlungsmethoden, die heutzutage im Alltag Anwendung finden. Auch das Vertrauen in eine Währung und deren Stabilität spielte und spielt nach wie vor eine zentrale Rolle und findet daher immer wieder Erwähnung.

2.1 Geschichte und Funktionen des Geldes

Das Geld, so wie wir es kennen, hat eine lange und bewegte Geschichte hinter sich und insbesondere die Form der Zahlungs- und Tauschmittel hat sich im Laufe der Jahrtausende stetig verändert. Sprechen wir heute von Geld, denkt jeder sofort an Münzen und Banknoten. Auch unsichtbares Geld auf den Bankkonten, sogenanntes Buch- oder Giralgeld, wird überall akzeptiert, da dem dahinterstehenden Wert vertraut wird.[6] Letztendlich ist Geld das, was in einer Gesellschaft als Zahlungs- und Tauschmittel akzeptiert wird. Durch eine Regelung im Rahmen einer Rechtsordnung entsteht die Verpflichtung, das Geld als gesetzliches Zahlungsmittel anzunehmen. Die Hoheit über die Schaffung und Verbreitung des Geldes haben dabei die Zentralbanken.[7]

Die ursprüngliche Form und der Anfang des Geldes ist das Warengeld, welches auch als Naturalgeld bezeichnet wird. Beispiele dafür sind Muscheln, Schmuck oder Felle.[8] Aufgrund des zunehmenden Handels wurden anschließend ca. im Jahr 700 vor Christus im antiken Königreich Lydien die ersten Münzen geprägt.[9] Dadurch entstand der enorme Vorteil, dass die einzelnen Gegenstände nicht mehr mühsam gewogen werden mussten, sondern einfach anhand der Anzahl der Münzen abgezählt werden konnten. Ausgehend von den ersten Prägungen im privaten Sektor übernahm das Königreich selbst die Prägungen, um für den Inhalt und Wert der Münze garantieren zu

6 Vgl. Deutsche Bundesbank (o. D.) (abgerufen am 10. Jul. 2018).

7 Vgl. Gabler Wirtschaftslexikon (2018) (abgerufen am 10. Jul. 2018).

8 Vgl. Deutsche Bundesbank (o. D.) (abgerufen am 11. Jul. 2018).

9 Vgl. Ellrich (2012) (abgerufen am 11. Jul. 2018).

können.[10] Auch hier spielte demnach schon das Vertrauen in die Währung eine wichtige Rolle, insbesondere um Fälschungen vorzubeugen, die so alt sind, wie das Geld selbst. Aber trotz allen Erfolges über viele Jahrhunderte hatten die Münzen auch entscheidende Nachteile. Die Materialien wie Gold und Silber waren selten und teuer und die Münzen konnten aufgrund ihres Gewichtes nicht in beliebiger Menge von einer Person transportiert werden.

Nicht zuletzt aus diesen Tatsachen entstand in China im neunten Jahrhundert nach Christus das erste Papiergeld.[11] Allerdings konnte sich diese neue Form des Geldes in Europa lange nicht durchsetzen, da im Gegensatz zu beispielsweise Silbermünzen hinter Papiergeld keinerlei Warenwert stand und schlichtweg das Vertrauen der Bevölkerung fehlte. Nicht zuletzt aufgrund der Vorteile der einfachen und günstigen Herstellung konnte sich das Papiergeld allerdings auch in Europa zunehmend durchsetzen.[12] Waren bis Mitte des 20. Jahrhunderts viele Währungen noch durch Gold oder andere Werte gedeckt, sind heute nahezu alle Währungen sogenannte Fiat-Währungen. Dies bedeutet, dass die Währungen durch keinerlei materiellen Wert gedeckt werden, sondern der Wert lediglich auf dem Umstand basiert, dass es als gesetzliches Zahlungsmittel anerkannt wird.[13]

Neben dem bereits vorgestellten Natural-, Münz- und Papiergeld ist das Giralgeld die heute wichtigste Art des Zahlungs- und Abrechnungsverkehrs. Ursprünglich wurde das Geld in die Kontobücher der (Giro)Banken eingetragen, damit Kaufleute anschließend Geld von Konto zu Konto bewegen konnten – daher auch die Bezeichnung als Buchgeld. Diese Aufzeichnung erfolgt heutzutage fast ausschließlich in digitaler Form. Das Giralgeld ist dabei kein gesetzliches Zahlungsmittel, genießt aber dennoch allgemeine Akzeptanz im Wirtschaftsleben, da es jederzeit wieder in Bargeld umgewandelt werden kann. Das Bargeld an sich macht heute nur noch einen geringen Anteil des im Umlauf befindlichen Geldes aus.[14] Beim Giralgeld verdeutlicht sich erneut, wie wichtig

10 Vgl. Rogoff (2016), S. 27.

11 Vgl. Ellrich (2012) (abgerufen am 11. Jul. 2018).

12 Vgl. Deutsche Bundesbank (o. D.) (abgerufen am 11. Jul. 2018).

13 Vgl. Grusch, Melingo (2012), S. 42 f.

14 Vgl. Deutsche Bundesbank (o. D.) (abgerufen am 11. Jul. 2018).

das Vertrauen in die jeweilige Währung ist. Während bei Münzgeld der Wert des Geldes noch im Warenwert (beispielsweise Gold oder Silber) lag, muss in modernen Zeiten von Banknoten und Giralgeld einfach darauf vertraut werden, dass das Geld seinen Wert behält und jederzeit gegen Waren eingetauscht werden kann. Um dieses Vertrauen zu stärken, wurden von Staaten Geldordnungen entwickelt, die beispielsweise ein gesetzliches Zahlungsmittel festlegen und vor Fälschungen schützen sollen.[15] Dieses Vertrauen wurde allerdings nicht zuletzt durch die Finanzkrise ab 2007 bei vielen Menschen auf eine harte Probe gestellt, sodass Zweifel und Skepsis gegenüber Veränderungen im Zahlungsverkehr zumindest nachvollziehbar sind.

In unseren modernen Wirtschaftskreisläufen wird Arbeit mit Geld anstatt mit Waren entlohnt.[16] Anhand dieses und der bereits genannten Beispielen aus der Geschichte wird unter wirtschaftlichen Gesichtspunkten zwischen drei Geldfunktionen unterschieden: Tauschmittelfunktion, Recheneinheitsfunktion sowie Wertaufbewahrungsfunktion.[17]

Die Tauschmittelfunktion erleichtert in erster Linie den Austausch der einzelnen Güter und Waren. Ein Austausch von Gütern ohne allgemein akzeptiertes Tauschmittel wäre deutlich komplizierter, da ansonsten ein Tauschvorgang nur stattfinden würde, wenn die Ware der anderen Person überhaupt benötigt wird. Eine moderne Wirtschaft würde ohne allgemein anerkanntes Gut, welches als Gegenleistung akzeptiert wird, zusammenbrechen.

Im Rahmen der Recheneinheitsfunktion werden durch Geld Güter wertmäßig vergleichbar. Um heutzutage bei der Vielzahl an Gütern die einzelnen Austauschverhältnisse bestimmen zu können, würde die zentral benötigte Rechenleistung für die Berechnung der Informationen ins Unermessliche steigen. Geld wird somit „die Grundlage jedes wirtschaftlichen Rechnungswesens und zur Voraussetzung von Wirtschaftlichkeits- und Rentabilitätsberechnungen“.[18]

---

15 Vgl. Deutsche Bundesbank (o. D.) (abgerufen am 11. Jul. 2018).

16 Vgl. Barfuß (1992), S. 1.

17 Vgl. hierzu und im Folgenden Siebert, Lorz (2007), S. 258 f.

18 Barfuß (1992), S. 2.

Die dritte Funktion des Geldes ist die Wertaufbewahrungsfunktion, die ermöglicht, dass erhaltenes Geld auch für eine zukünftige Transaktion zurückgelegt werden kann und nicht direkt wieder zum Kauf eines Gutes verwendet werden muss. Mit anderen Worten ist es dadurch möglich, Geld zu sparen und Ware gegen Tauschbereitschaft zu tauschen, beispielsweise Güter zu veräußern und den Gegenwert erst zukünftig zu erhalten. Somit wird das Geld zu einem Mittler zwischen Vergangenheit, Gegenwart und Zukunft. Diese Funktion ist aber an die Beständigkeit des Geldes gebunden. Verschlechtert sich der Wert des Geldes, so ist auch automatisch die Wertaufbewahrungsfunktion davon betroffen.[19] Insbesondere diese Funktion ist bei Kryptowährungen oft nicht erfüllt, da der Kurs und somit der Wert der Kryptowährung starken Schwankungen ausgesetzt ist.

2.2 Aktuelle Zahlungsmethoden

Bevor der Fokus weiter auf die Blockchain-Technologie und Kryptowährungen rückt, wird zunächst ein Überblick über die heutzutage genutzten Zahlungsmethoden geschaffen. Dies ist relevant, da sich für die Akzeptanz einer neuen Technologie und Währung zuerst Fragen nach der Verbesserung des Status Quo und nach sinnvollen Anwendungsfeldern stellen.

Folgende Zahlungsmethoden sind heutzutage von Relevanz: Bargeld, Vorkasse, Rechnung, Nachnahme, Lastschrift, Kreditkarte und PayPal.

Die Zahlungsmethoden, die nicht über das Internet abgewickelt werden können, verlieren in der relevanten und zahlungskräftigen Zielgruppe zunehmend an Bedeutung. Bereits im Jahr 2016 nutzten 74 Prozent aller 25- bis 34-Jährigen Online-Banking für ihre Transaktionen. Zudem gibt es einen Zusammenhang zwischen steigendem Nutzergrad und höherem Bildungsgrad beziehungsweise höherem Haushaltseinkommen.[20] Diese Zielgruppe zeigt sich oft offener gegenüber neuen Technologien. Speziell das Bargeld wird uns aber in gewissen Teilen noch lange erhalten bleiben, obwohl technisch gesehen eine bargeldlose Gesellschaft längst umsetzbar wäre und der

[19] Vgl. Ehrlicher (1982), S. 377.

[20] Vgl. Statistisches Bundesamt (2017) (abgerufen am 19. Jul. 2018).

Wechsel weniger Aufwand bedeuten würde, als beispielsweise die Währungsumstellung auf den Euro.[21] Auch weitere Punkte, wie unter anderem der Aspekt der Kosten der Bargeldversorgung und die Möglichkeit der schnelleren Bezahlung würden für eine bargeldlose Gesellschaft sprechen.[22] Nichtsdestotrotz vertrauen insbesondere die Deutschen immer noch dem Bargeld. Dies zeigt eine auch Statistik einer Bundesbank-Studie aus dem Jahr 2017. Demnach wurden rund 75 Prozent der Einkäufe mit Bargeld bezahlt. Diese Zahl ist sogar noch deutlich höher, je weiter die Beträge unter 50 Euro liegen.[23] Als Gründe dafür wurden neben der besseren Ausgabenkontrolle und den Sicherheitsbedenken auch die Anonymität genannt. Viele Menschen befürchten, dass ihr Konsumverhalten dadurch komplett transparent für Staat und Unternehmen wird.[24]

Die Zahlung per Vorkasse gehört zu den klassischen Zahlungsmethoden, besitzt aber im heutigen elektronischen Handel (E-Commerce) durchaus noch Relevanz. Hierbei überweist der Käufer das Geld unmittelbar nach Kaufbestätigung und Erhalt der Kontodaten. Erst dann verschickt der Verkäufer die Ware.[25]

Der Kauf auf Rechnung läuft anfänglich genauso ab, wie der Kauf per Vorkasse und zählt zu den beliebtesten Zahlungsmethoden im E-Commerce.[26] Nach der Kaufbestätigung versendet der Verkäufer die Ware und verschickt per E-Mail und/oder beiliegend im Paket die Rechnung inklusive Zahlungsziel. Der Käufer kann somit die Ware erst begutachten und braucht nur das zu bezahlen, was er tatsächlich behält.

Bei der Zahlungsvariante per Nachnahme erfolgt die Bezahlung direkt beim Erhalt der Ware. Entrichtet wird der fällige Betrag dabei an den Paketdienst oder in der Postfiliale. Dabei entsteht eine Nachnahmegebühr, die im Normalfall vom Verkäufer an den Käufer weitergegeben wird. Neben den Zusatzkosten entsteht für den Käufer zudem der Zwang, zum Lieferzeitpunkt zu Hause zu sein.[27]

---

21 Vgl. Hungerland et al. (2017), S. 8 (abgerufen am 19. Jul. 2018).

22 Vgl. Hungerland et al. (2017), S. 11 (abgerufen am 19. Jul. 2018).

23 Vgl. Deutsche Bundesbank (2018) (abgerufen am 19. Jul. 2018).

24 Vgl. Frankfurter Allgemeine Zeitung A (2018) (abgerufen am 19. Jul. 2018).

25 Vgl. Dannenberg, Ulrich (2004), S. 73.

26 Vgl. Kalt (2018) (abgerufen am 31. Jul. 2018).

27 Vgl. Dannenberg, Ulrich (2004), S. 71 f.

Eine weitere, weit verbreitete Zahlungsmethode im E-Commerce ist die Zahlung per Lastschrift. Diese Methode ist für Käufer sowie Verkäufer relativ unproblematisch und bequem. Der Käufer gibt normalerweise per Online-Formular seine Kontodaten an und ermächtigt somit den Verkäufer, den jeweils fälligen Betrag einziehen zu dürfen. Der Verkäufer übermittelt die Lastschrift an sein Kreditinstitut, welches diese wiederum an die Bank des Käufers weiterleitet. Anschließend wird das Konto des Käufers belastet und dem Verkäufer wird das Geld gutgeschrieben.[28] Besonders oft wird das Lastschriftverfahren bei regelmäßig wiederkehrenden Zahlungen, wie beispielsweise Abonnements und Mietzahlungen, verwendet.[29]

Insbesondere bei internationalen Geschäften ist die Zahlung per Kreditkarte beliebt und wird beim weltweiten elektronischen Zahlungsverkehr mit Abstand am häufigsten genutzt. Deutschland zählt noch zu den Ausnahmen, jedoch steigen die Nutzerzahlen jährlich.[30] Die in Deutschland beliebtesten Kreditkartenorganisationen sind hierbei Visa und Mastercard. Bei der Kaufabwicklung gibt der Kreditkarteninhaber (der Käufer) im ersten Schritt seine Kreditkartendaten (Kartennummer, Gültigkeitsdatum, Kartenprüfnummer) in ein Online-Formular ein. Anschließend werden die Daten an die kreditkartenbetreuende Stelle (Kreditkartenacquirer) des Verkäufers weitergeleitet, der die weitere Zahlung abwickelt und dafür sorgt, dass der Verkäufer sein Geld bekommt.[31] Die aktuell in Deutschland gebräuchlichste Form der Kreditkarte ist die Charge-Karte.[32] Dabei werden die getätigten Käufe zu einer Gesamtsumme aufgerechnet und beispielsweise einmal monatlich vom Konto abgebucht.[33] Die Beliebtheit liegt nicht zuletzt daran, dass durch diese Form dem Kunden bis zum nächsten Abrechnungszeitpunkt ein kurzfristiges, zinsloses Darlehen gewährt wird.

Für den stark wachsenden E-Commerce-Bereich wurden einige der bereits erwähnten Zahlungsmethoden zum Teil angepasst. Darüber hinaus wurden auch komplett neue

28 Vgl. Dannenberg, Ulrich (2004), S. 127.

29 Vgl. Kalt (2018) (abgerufen am 01. Aug. 2018).

30 Vgl. Dannenberg, Ulrich (2004), S. 78.

31 Vgl. Stahl et al. (2012), S. 4-13.

32 Vgl. Wiesner (2018) (abgerufen am 01. Aug. 2018).

33 Vgl. Dannenberg, Ulrich (2004), S. 78.

Verfahren zur elektronischen Bezahlung (E-Payment) entwickelt. Als Beispiel in diesem Fall soll der Bezahldienst PayPal dienen. Daneben gibt es aber auch noch nutzerkontounabhängige Methoden wie die paysafecard oder Direktüberweisungsverfahren wie giropay.[34]

PayPal kam bereits im Jahr 1999 auf den Markt und ist inzwischen eines der erfolgreichsten Zahlungssysteme im Internet.[35] Die Zielsetzung ist nach wie vor, den Bezahlvorgang für den Kunden so einfach und zugänglich wie möglich zu gestalten. Stand 2018 gibt es ungefähr 237 Millionen aktive Kunden.[36] PayPal bietet darüber hinaus neben Schnelligkeit, unkompliziertem Ablauf und Datensicherheit auch den sogenannten Käuferschutz. Dadurch sind Käufer, die per PayPal bezahlen, abgesichert, falls der gekaufte Artikel gar nicht, beschädigt oder anders als beschrieben ankommt.[37]

2.3 Zahlungsverkehr im digitalen Wandel

Die Digitalisierung schreitet in allen Bereichen von Gesellschaft und Wirtschaft weiter voran. Die Beispiele reichen von Industrie 4.0 über neuronale Netze bis hin zur Tatsache, dass im Jahr 2018 ungefähr 57 Millionen Menschen in Deutschland ein Smartphone nutzen.[38] Dieser digitale Wandel beeinflusst auch das Zahlungsverhalten sowie die Zahlungsmethoden. Im kontaktlosen oder mobilen Bezahlen zeichnet sich dieser Wandel bereits ab – allerdings vergehen zwischen Initiierung und Buchung der Zahlung oft mehrere Stunden.[39] Insbesondere in der Wirtschaft besteht der Bedarf nach Zahlungsabwicklungen in Echtzeit, die einfacheres Liquiditätsmanagement und Risikoverminderung bedeuten.[40]

Ausgehend von den Unterkapiteln 2.1 und 2.2 lässt sich festhalten, dass die erwähnten und nahezu alle anderen Zahlungsmethoden in irgendeiner Form von Banken und zentralen Institutionen abhängig sind. Dies gilt im gleichen Maße für viele Zahlungsmethoden, die durch die Digitalisierung entstanden sind und entstehen werden.

---

34 Vgl. Stahl et al. (2012), S. 4-15 f.

35 Vgl. Dannenberg, Ulrich (2004), S. 167.

36 Vgl. PayPal A (o. D.) (abgerufen am 02. Aug. 2018).

37 Vgl. PayPal B (o. D.) (abgerufen am 02. Aug. 2018).

38 Vgl. Statistisches Bundesamt (2018) (abgerufen am 06. Aug. 2018).

39 Vgl. Deutsche Bundesbank (2017) (abgerufen am 07. Aug. 2018).

40 Vgl. Atzler (2018) (abgerufen am 07. Aug. 2018).

Dadurch ergibt sich zwar eine gewisse Sicherheit und Beständigkeit, auf der anderen Seite besteht eben eine komplette Abhängigkeit, nicht zuletzt auch bei Sicherheitsaspekten. Somit können einige Wenige auf viele Menschen und deren Geld gewaltigen Einfluss nehmen.

Durch die Nullzinspolitik, bei der Sparer bei gleichzeitiger Inflation Geld verlieren, und den ungezügelten Spekulationsgeschäften an den Finanzmärkten, fingen einige Menschen an zu überlegen, wie eine möglichst sichere, einfach und unabhängig übertragbare sowie inflationsfreie Währung ohne staatliche Kontrolle aussehen könnte.[41] Zudem wurde eine transparente und verlässliche Technologie benötigt, die die eben genannten Eigenschaften sicherstellen kann. Dies war die Geburtsstunde der Kryptowährungen.

Noch werden Kryptowährungen von vielen sehr skeptisch betrachtet. Trotz steigendem Bekanntheitsgrad des Begriffes wissen viele Menschen nahezu nichts über Hintergründe und Technologie. Auch die zuletzt stark schwankenden Kurse, beispielsweise des Bitcoins, haben die Vorbehalte verstärkt.[42] Viele denken zudem im Zusammenhang mit Bitcoin oft an die dunklen Seiten des Internets, beispielsweise an anonyme, illegale Geschäfte, Betrug oder gehackte Benutzer, die nahezu ihre gesamte Existenz verloren haben. Dabei wird gerne ausgeblendet, dass auch mit den herkömmlichen Zahlungsmethoden vielfach illegale Machenschaften stattfinden.[43] Der Bekanntheitsgrad dürfte demnach deutlich über dem Anteil der tatsächlichen Nutzung liegen. Falls Deutsche investieren, liegt nach wie vor Gold an erster Stelle und Kryptowährungen werden von der Mehrheit eher als Nischenprodukt betrachtet.[44]

Interessant dabei ist allerdings, wieso neue Zahlungsmethoden und -systeme anfänglich oft viel Skepsis erfahren und eine hohe Vertrauenshürde besteht. Viele dieser Methoden, beispielsweise kontaktloses Bezahlen, würden nach kurzer Eingewöhnung das alltägliche Leben einfacher machen. Diese Vertrauensvorbehalte sind bei der Nutzung von Facebook, Google oder des Smartphones deutlich geringer, obwohl dort

41 Vgl. Heun (2018), S. 35.

42 Vgl. Frankfurter Allgemeine Zeitung (2017) (abgerufen am 07. Aug. 2018).

43 Vgl. Rosenberger (2018), S. 14.

44 Vgl. Crypto Magazin (2018) (abgerufen am 07. Aug. 2018).

auch persönliche Daten angegeben werden und deren Umgang mit diesen zumindest als fragwürdig angesehen werden kann.[45] Stattdessen werden insbesondere die Kryptowährungen oft als zu kompliziert oder unzugänglich bezeichnet. Dies ist derzeit in Teilen auch noch der Fall, aber zumindest die Grundlagen sollten Interesse wecken, da nicht ohne Grund von vielen Experten die Kryptowährungen und die dahinterliegende Blockchain-Technologie als Zukunft angesehen werden.[46] Vielmehr würden Bezeichnungen wie kryptisch oder intransparent auf das aktuelle Geldsystem zutreffen. Wer weiß schon, dass Banken Geld durch Kreditvergabe quasi aus dem Nichts schaffen? Wer kennt die genaue Rolle der Zentralbanken und die Eigentümerstrukturen dahinter? Diese Argumente kommen insbesondere zum Tragen, wenn im Zusammenhang von Kryptowährungen oft kritisiert wird, dass das Geld aus dem Nichts geschaffen wird und dort keinerlei physisches Vermögen hinter liegt. Bei dem herkömmlichen Währungssystem geschieht dies analog, lediglich gesteuert und überwacht von Banken. Wirklich hinterfragt wird dies heutzutage von den Wenigsten. Nichtsdestotrotz funktioniert das Geldsystem in der jetzigen Form noch relativ gut und die Vertrauensgrundlage besteht weiterhin.[47]

Trotz aller bisherigen Skepsis und Kritik hat der Handel mit Kryptowährungen insbesondere in den letzten zwei Jahren einen regelrechten Boom erfahren. Derzeit gibt es 1.818 Kryptowährungen mit einer Gesamtmarktkapitalisierung von knapp 192 Milliarden Euro (Stand 13. Aug. 2018).[48] Die Gesamtmarktkapitalisierung ist dabei der Wert des gesamten Marktes und berechnet sich aus dem Produkt des Kurses der Coins und den Anteilen, die sich auf dem Markt im Umlauf befinden.[49] Der Bitcoin ist demnach zwar die bekannteste und wertmäßig wertvollste Kryptowährung, es gibt darüber hinaus aber noch viele andere, die durchaus Relevanz besitzen.

Um den Wertzuwachs und auch die Wertschwankungen zu verdeutlichen, zeigt die folgende Grafik beispielhaft den Kursverlauf des Bitcoins:

---

45 Vgl. Rosenberger (2018), S. 14.

46 Vgl. Schreder (2018), S. 17 ff.

47 Vgl. Koenig (2017), S. 14 f.

48 Vgl. CoinMarketCap A (o. D.) (abgerufen am 13. Aug. 2018).

49 Vgl. Cointrend (2017) (abgerufen am 13. Aug. 2018).

Abb. 1: Kursverlauf Bitcoin vom 01. Jan. 2017 bis 13. Aug. 2018
(Quelle: CoinMarketCap B (o. D.) (abgerufen am 13. Aug. 2018)).

Die Verläufe der Altcoins, die im Kapitel 4 vorgestellt werden, sehen dabei ähnlich aus. Wie zu sehen ist, stürzten der Bitcoin und andere Kryptowährungen zuletzt stark ab und es wurden Hunderte Milliarden Euro vernichtet. Lag der Kurs für einen Bitcoin im Dezember 2017 noch deutlich über 15.000 Euro, liegt der Kurs aktuell bei lediglich knapp über 5.500 Euro (Stand 19. Aug. 2018).[50] Es könnte der Verdacht entstehen, dass es sich hier lediglich um eine Spekulationsblase handelt, die nach einiger Zeit genauso schnell verschwindet, wie sie entstanden ist. Auf viele Kryptowährungen dürfte dies auch zutreffen. Der Bitcoin und auch eine Vielzahl der Altcoins werden von vielen nicht als Währung der Zukunft betrachtet und niemand weiß, welche Kryptowährungen in fünf Jahren relevant sein werden. Es ist aber davon auszugehen, dass die aktuellen Kryptowährungen mit hoher Wechselkursvolatilität, insbesondere im wirtschaftlichen Kontext, keine Zukunft haben. Zudem ist aktuell der Bitcoin als Zahlungsmittel im gesellschaftlichen Leben in Deutschland noch denkbar ungeeignet. Nur wenige Geschäfte in großen Städten und Ballungsräumen akzeptieren Bitcoins als Zahlungsmittel; oft handelt es sich dabei auch nur um Nischenprodukte oder Online-Lieferdienste.[51]

Vielmehr dürfen diese Verläufe als Trend und kommenden Paradigmenwechsel verstanden werden. Freie, private und dezentrale Währungen treten in Konkurrenz zu

50 Vgl. Stocker (2018) (abgerufen am 19. Aug. 2018).

51 Vgl. Hungerland et al. (2017), S. 20 (abgerufen am 13. Aug. 2018).

dem alten, zentralistischen Geldsystem.[52] Das Weltwirtschaftsforum schätzt, dass im Jahr 2025 etwa zehn Prozent des weltweiten Bruttoinlandproduktes in Form von Kryptowährungen auf Blockchains gespeichert sein wird.[53] Ein radikaler Umbruch bei der Nutzung von Zahlungsmethoden steht uns dabei aller Voraussicht nach allerdings nicht bevor – vielmehr sind dies die ersten Schritte einer langfristigen Entwicklung.

Doch bei dem aktuellen Wandel stellen sich auch berechtigte Fragen. Treten Kryptowährungen wirklich in Konkurrenz zu den klassischen Zahlungsmethoden und wollen diese zukünftig in jedem Bereich der Wirtschaft ersetzen? Ist dies überhaupt sinnvoll? Wie kann den Vorbehalten gegenüber neuen Technologien und Zahlungsmethoden, die sich nahezu durch die gesamte Geschichte des Geldes ziehen, entgegnet werden? Welche rechtlichen Grundlagen müssen geschaffen werden? Es darf bezweifelt werden, dass die zukünftige Anwendung von Kryptowährungen in der Bezahlung von Brötchen beim Bäcker liegt. Vielmehr ist die eigentliche Aufgabe, diese mit gewaltigem Potenzial gesegnete Technologie in die richtigen operativen Anwendungsfelder zu bringen, in denen sie ihren Nutzen entfalten kann. Ein Beispiel dafür könnten die sogenannten Smart Contracts (Intelligente Verträge) sein, die im Laufe dieser Thesis ausführlicher behandelt werden. Weitere anwendungsspezifische Chancen und Potenziale werden im Rahmen des Kapitels 7 vorgestellt.

[52] Vgl. Koenig (2017), S. 16.

[53] Vgl. Koenig (2017), S. 17 f.

3 Die Blockchain-Technologie

Aufbauend auf der Entwicklung des Geldes und des digitalen Wandels im Zahlungsverkehr beschäftigt sich dieses Kapitel ausführlich mit der Blockchain-Technologie, die die technische Grundlage fast aller Kryptowährungen darstellt.[54] Dabei werden die technischen Grundlagen, Funktionsweise sowie das kryptografische Verfahren näher betrachtet.

Das Konzept der Blockchain, wie diese im Rahmen der Kryptowährungen betrachtet wird, geht auf das Pseudonym Satoshi Nakamoto zurück, der im Jahr 2008 ebenfalls die Kryptowährung Bitcoin erfand. Nach den Anfängen des Bitcoins entstand das Problem, dass eine digitale Münze im Gegensatz zu physischen Münzen theoretisch unendlich oft vervielfältigt werden konnte. Dies wird auch als Double Spending Problem bezeichnet. Bei herkömmlichen Transaktionsgeschäften lässt sich eine Mehrfachausgabe nur durch die Führung durch zentrale Stellen vermeiden, beispielsweise einer Bank. Um eben dieser Abhängigkeit zu entgehen und trotzdem Sicherheit gewährleisten zu können, erfand Nakamoto die Blockchain in ihrer jetzigen Form.[55] Dadurch löste er das Problem, dass Menschen, die sich gegenseitig nicht vertrauen, trotzdem zu einem Konsens kommen können.[56] Darüber hinaus nimmt die Blockchain durch ihre Dezentralität die Notwendigkeit, Banken oder Regierungen vertrauen zu müssen.[57] Auch hier läuft demnach vieles auf Vertrauen als einen der ausschlaggebenden Punkte hinaus. Das Vertrauen gegenüber Personen ist nicht mehr notwendig, vertraut werden muss lediglich den komplexen Algorithmen der Blockchain. Zudem ist das System jederzeit für alle Personen öffentlich zugänglich. Nicht zuletzt aufgrund dieser Punkte wird die Blockchain-Technologie von einigen als technische Revolution oder sogar als größte digitale Erfindung des 21. Jahrhunderts bezeichnet.[58]

---

54 Vgl. Toggweiler (2017) (abgerufen am 19. Jul. 2018).

55 Vgl. Glücklich A (2017), S. 13 f.

56 Vgl. Koenig (2017), S. 34 f.

57 Vgl. Glücklich A (2017), S. 15.

58 Vgl. Giese et al. (2017), S. 55.

Neben der Anwendung als Grundlage vieler Kryptowährungen bietet die Blockchain Potenzial, um sich auch in anderen Bereichen in Kombination mit der finanziellen Abwicklung über Kryptowährungen zu einem leistungsstarken Werkzeug zu entwickeln. Beispiele dafür sind Anwendungsfelder in der Finanzindustrie, im Supply Chain Management oder auch bei der Aufzeichnung und Übertragung von Immobilien.[59]

Die Blockchain kann definiert werden als ein digitales, dezentrales Kassenbuch, in dem Transaktionen, beispielsweise einer Kryptowährung, in Blöcken gespeichert und öffentlich sichtbar gemacht werden. Ist ein Block voll, wird einfach ein neuer Block an die Blockkette angefügt. Dabei werden die bisher entstandenen Blöcke nicht überschrieben, sondern bleiben unverändert bestehen.[60] Folgendes Schema demonstriert vereinfacht den Aufbau einer Blockchain:

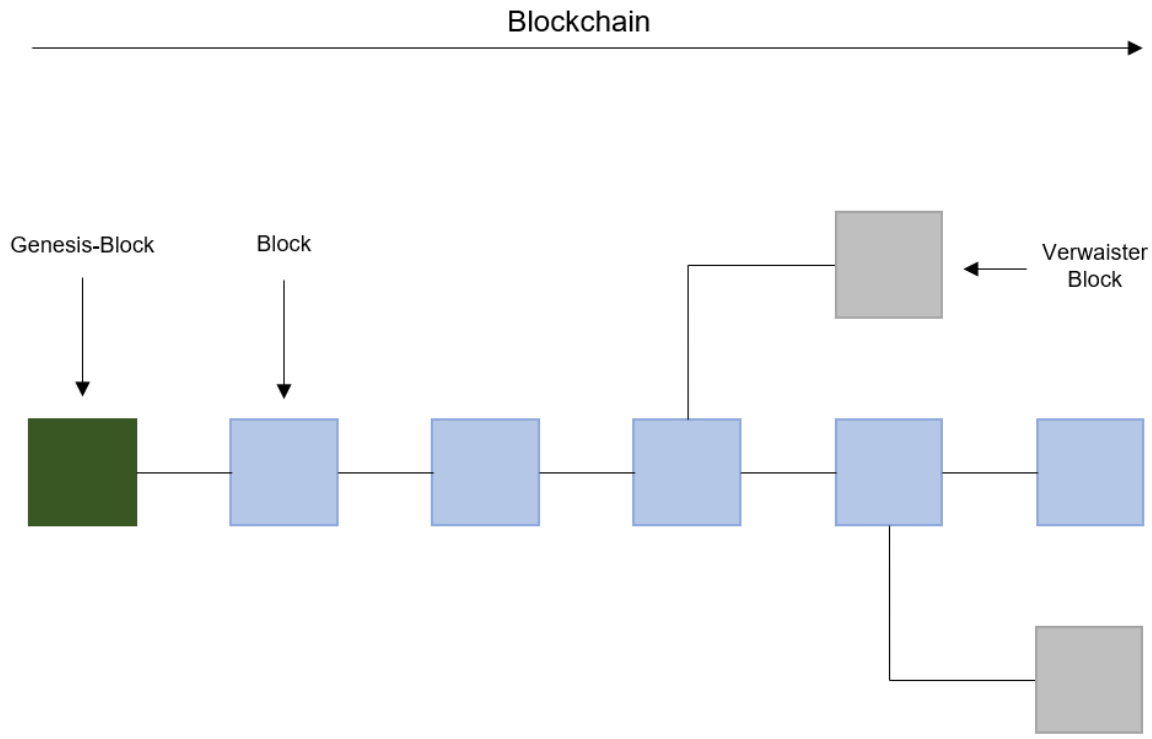

Abb. 2: Vereinfachtes Schema einer Blockchain

(Quelle: Eigene Darstellung nach Blockchainwelt A (2018) (abgerufen am 16. Aug. 2018)).

[59] Vgl. Heun (2017), S. 133.

[60] Vgl. Heun (2018), S. 125.

Der Genesis-Block (grün) ist der erste Block innerhalb einer Blockchain. In der Nummerierung zählt er als Block Null und ist nahezu immer direkt in die Anwendung eingebunden, die die Blockchain nutzt.[61] Die hellblauen Blöcke stellen die regulären, gültigen Blöcke innerhalb einer Blockchain dar und werden aus diversen Transaktionen gebildet. Diese sind miteinander verbunden und durch eine spezielle Kryptografie abgesichert, sodass dort im Nachhinein nichts mehr verändert werden kann. Dazu beinhaltet jeder erstellte Block einen sogenannten Hash aus dem vorherigen Block.[62] Es kann zudem vorkommen, dass Blöcke verwaisen (grau). Dies geschieht, wenn nahezu gleichzeitig zwei gültige Blöcke erzeugt werden. In der Regel wird dann der erste empfangene Block übernommen, während der zweite Block abgezweigt wird. Es findet somit keine weitere Verkettung mehr statt.[63]

3.1 Funktionsweise der Blockchain

Das grundlegende Schema der Blockchain wurde in Kapitel 3 kurz dargestellt. Allerdings passiert innerhalb der Blockchain noch einiges mehr, wodurch verdeutlicht wird, wie innovativ und sicher diese Technologie tatsächlich ist. Theoretisch gibt es durch die Anzahl an Kryptowährungen viele verschiedene Blockchains. Die folgenden Erklärungen beziehen sich beispielhaft auf das Bitcoin-Netzwerk. Da einige Erklärungen zur Blockchain durchaus komplex und mathematisch sind, wird versucht, das aktuelle Kapitel auch für Personen ohne Vorwissen möglichst verständlich zu gestalten.

Der allererste Schritt ist im Regelfall die Transaktion zwischen zwei Personen. Bevor diese Transaktion aber überhaupt stattfinden kann, müssen beide Personen eine sogenannte Wallet (digitale Geldbörse) einrichten.[64] Vergleichbar ist diese Wallet mit einem Bankkonto, allerdings müssen zum Eröffnen keinerlei persönliche Daten angegeben werden. Die Wallet kann dabei per Website oder spezieller Software selbst erstellt werden. Nach der Erstellung erhält die erstellende Person zwei mathematisch zusammenhängende, kryptografische Schlüssel – den privaten und den öffentlichen Schlüssel (Private Key und Public Key). Vergleichbar ist der öffentliche Schlüssel mit der

61 Vgl. Blockchainwelt A (2018) (abgerufen am 16. Aug. 2018).

62 Vgl. Giese et al. (2017), S. 57.

63 Vgl. Heun (2018), S. 126.

64 Vgl. Mago, Gillen (2016), S. 15.

International Bank Account Number (IBAN), während der private Schlüssel der eigenen Persönlichen Identifikationsnummer (PIN) entspricht.[65] Der öffentliche Schlüssel ist sozusagen die Adresse der Wallet und kann ohne Bedenken weitergegeben werden. Niemals weitergegeben werden darf hingegen der private Schlüssel, da durch diesen der volle Zugriff auf alle in der Wallet befindlichen Bitcoin-Adressen gewährt wird.[66] Möchte ich im Rahmen einer Transaktion nun Person X einen Bitcoin überweisen, brauche ich dazu den öffentlichen Schlüssel von X. In der Transaktion, beziehungsweise später in der Blockchain, steht dabei nicht Person X, sondern diese Person bleibt anonym. Stattdessen taucht dort eine Adresse auf, die, bestehend aus 34 Zahlen und Buchstaben, entweder mit einer Eins oder mit einer Drei beginnt. Zum Beispiel:

1HFSx5TPYYzQTQmBXeJNcMhUHT6FNGF11q[67]

Wie der kryptografische SHA256-Algorithmus dahinter funktioniert, wird in Unterkapitel 3.4 veranschaulicht. Der öffentliche Schlüssel erfüllt dabei neben der Möglichkeit, Coins an diese Adresse senden zu können, auch die Funktion, dass jeder Kontostand jederzeit eingesehen werden kann – jedoch, wie bereits erwähnt, anonym, beziehungsweise pseudonymisiert.[68]

In der Transaktion wird anschließend folgendes verzeichnet: Die Absenderadresse (mein öffentlicher Schlüssel), die Menge an Bitcoins (1 BTC) sowie die Empfängeradresse (öffentlicher Schlüssel von Person X).[69] Ein Beispiel (in diesem Fall mit der Bitcoinmenge 8,62) könnte in einer Wallet wie folgt aussehen:

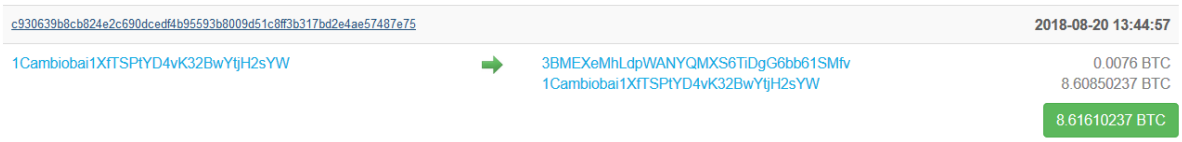

Abb. 3: Bitcoin-Transaktion

(Quelle: Blockchain (2018) (abgerufen am 20. Aug. 2018)).

65 Vgl. Koenig (2017), S. 33.

66 Vgl. Stein (2017) (abgerufen am 20. Aug. 2018).

67 Vgl. Hosp (2017), S. 48.

68 Vgl. Stein (2017) (abgerufen am 20. Aug. 2018).

69 Vgl. Giese et al. (2017), S. 66.

Um diese Transaktion durchführen zu können, bedarf es einer Art Signatur, die sicherstellt, dass ich den einen Bitcoin in diesem Fall auch tatsächlich versenden kann. Wichtig dabei ist, dass Bitcoins nicht in der Wallet selbst gespeichert werden, sondern weiterhin auf der Blockchain liegen. In der Wallet liegen lediglich die mathematisch mit dem öffentlichen Schlüssel verbundenen privaten Schlüssel. Hat jemand zu einem vorherigen Zeitpunkt einen Bitcoin an meinen öffentlichen Schlüssel gesendet, kann der private Schlüssel in meiner Wallet dazu eine digitale Signatur erstellen, mit der der Bitcoin dann an die Person X versendet werden kann. Einfach gesagt: Der Bitcoin kann versendet werden, sobald ich einen privaten Schlüssel zu einem öffentlichen Schlüssel besitze.[70] Im Netzwerk wird dann geprüft, ob die digitale Signatur und die angegebenen Bitcoins zusammenpassen, also ob es sich um eine korrekte und gültige Transaktion handelt. Dies ist notwendig, da es sich bei diesem Beispiel Bitcoin um eine Open-Source-Software handelt, das heißt, der eigentliche Code ist für jeden öffentlich abrufbar.[71]

Hier kommt nun das sogenannte Mining ins Spiel. Das Mining ist ein Vorgang, der im Zusammenhang mit Kryptowährungen aufgrund des Namens oft falsch verstanden wird. Es handelt sich dabei um durch Computerhardware durchgeführte, mathematische Berechnungen, die die Sicherheit erhöhen und Bitcoin-Transaktionen bestätigen.[72] Dabei wird folgendes geprüft:

- Ist die digitale Signatur des Absenders korrekt?
- Verfügt der Absender über genügend Coins, um diese Transaktion durchführen zu können?
- Ist die Adresse des Empfängers korrekt?[73]

Viele glauben allerdings, dass durch Mining lediglich neue Kryptowährungen erzeugt (gemined) werden – diese Annahme ist aber größtenteils nicht korrekt.[74] Grundsätzlich kann jede am Netzwerk beteiligte Person zum Miner werden und somit die Aufgabe

70 Vgl. Roos (2018) (abgerufen am 22. Aug. 2018).

71 Vgl. Hosp (2017), S. 51.

72 Vgl. Bitcoin (o. D.) (abgerufen am 22. Aug. 2018).

73 Vgl. Koenig (2017), S. 37.

74 Vgl. Hosp (2017), S. 54.

übernehmen, die im regulären System bisher die Banken haben.[75] Das Transaktionsbeispiel wird nun zusammen mit weiteren, mehreren Hundert unbestätigten Transaktionen in einem Block zusammengefasst. Anschließend versuchen, die im dezentralen System beteiligten Miner, die dahinterliegende mathematische Aufgabe am schnellsten zu lösen, um die Transaktionen zu bestätigen. Dazu muss ein gültiger, sogenannter Hash gefunden werden, der unter der vorher festgelegten Referenzzahl liegt. Das Finden des gültigen Wertes basiert auf einem reinen Zufallsprinzip und ist vergleichbar mit Lotto spielen. Normalerweise ist die Hashberechnung durch einen Computer kein Problem. Die Schwierigkeit und Notwendigkeit enormer Rechenkapazität wird durch eine künstliche Erhöhung der Schwierigkeit (Difficulty) erreicht, indem Hashes mit einer bestimmten Anzahl von Nullen beginnen müssen. Je mehr Nullen, desto schwieriger wird es, den richtigen Hash zu erraten.[76] Dies ist notwendig, da sonst in kürzester Zeit alle der auf insgesamt 21 Millionen begrenzten Bitcoins bereits erzeugt worden wären.[77]

Da die Miner die Transaktionen innerhalb des Blockes nicht verändern dürfen, greifen sie auf einen anderen Datensatz zurück, auf die sogenannte Nonce. Dieser Datensatz wird nun so lange verändert, bis der Hash das gewünschte Format findet. Format bedeutet in diesem Fall nichts anderes, als dass der Hash die vom Bitcoin-Protokoll festgelegte Anzahl Nullen an erster Stelle hat. Der Rest der Zeichen spielt dabei keine Rolle mehr.[78] Ein Knoten entdeckt alle zehn Minuten die Lösung des Problems und übermittelt die Lösung an das Netzwerk, welches wiederum die Lösung erneut prüft und bestätigt.[79] Diese zehn Minuten sind festgelegt und die Schwierigkeit wird mit der Zeit dahingehend angepasst.

Ist eine Transaktion nun Teil eines gültigen Blocks, wird diese innerhalb von Millisekunden bestätigt, da mehrere Millionen Knoten gleichzeitig diesen Block kopieren und dieser nun als Ausgangspunkt für einen weiteren Block gilt. Wird die mathematische Aufgabe bildlich als Puzzle dargestellt, dauert die Bestätigung, ob ein Puzzle korrekt

---

75 Vgl. Koenig (2017), S. 37.

76 Vgl. Zoller (2017) (abgerufen am 22. Aug. 2018).

77 Vgl. Blockchainwelt B (2018) (abgerufen am 22. Aug. 2018).

78 Vgl. BTC-Echo A (o. D.) (abgerufen am 22. Aug. 2018).

79 Vgl. Berger (2015) (abgerufen am 22. Aug. 2018).

ist, meist nur Sekunden, während die Fertigstellung des Puzzles Stunden oder Tage dauern kann. Ähnlich verhält es sich hier mit der Erstellung und Bestätigung eines Blocks.[80] Der Miner, der die Lösung gefunden und somit den Block erstellt hat, erhält dafür eine Belohnung, dass er seine Rechenkapazität sowie Hardware zur Verfügung gestellt hat. Dabei handelt es sich um die Summe aller Transaktionsgebühren der im Block enthaltenden Transaktionen, zuzüglich derzeit 12,5 Bitcoins.[81] Das hierfür zugrundeliegende Konsens-Verfahren zur Bestätigung (Konsens in dem Sinne, dass sich alle Nutzer der Blockchain darauf verständigen, dass der bestätige Block und dessen Transaktionen gültig sind und dieser für alle der gleiche ist) heißt Proof-of-Work (PoW, zu Deutsch: Arbeitsnachweis) und wird im Unterkapitel 3.2 zusammen mit anderen Verfahren näher erläutert.

Bildlich sieht die Verkettung innerhalb einer Blockchain in etwa wie folgt aus:

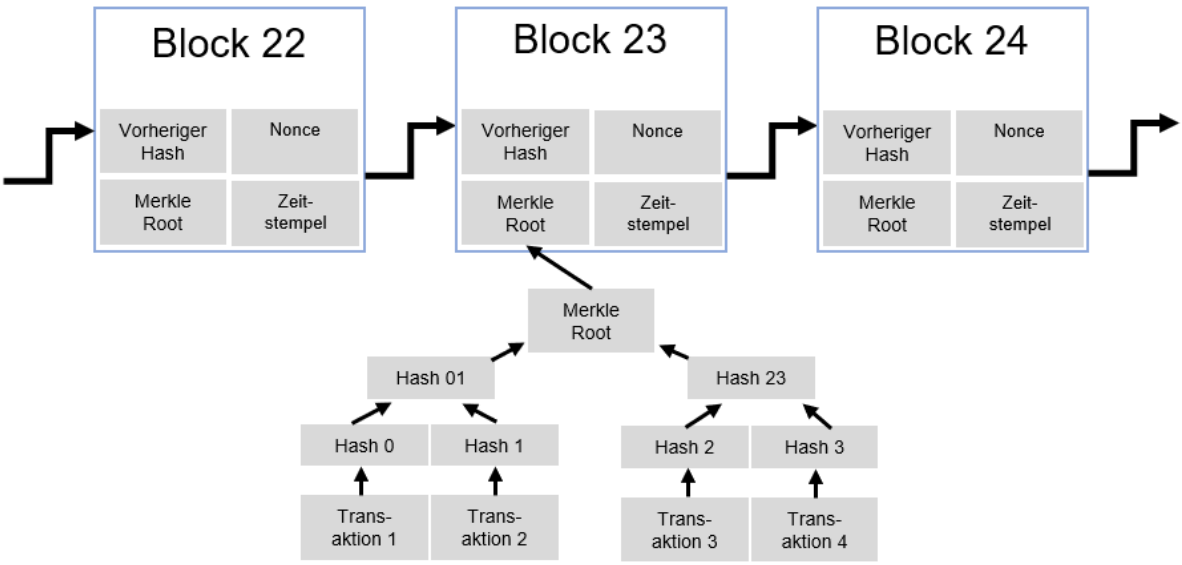

Abb. 4: Bestandteile eines Blocks

(Quelle: Eigene Darstellung nach Decentralbox (2017) (abgerufen am 27. Aug. 2018)).

Jeder neue, bestätigte Block verweist unwiderruflich auf den Block davor. Dies geschieht, indem in jeder Kopfzeile (Header) eines neuen Blockes der Hash aus dem vorherigen Block eingetragen wird. Dadurch entsteht eine unveränderliche Kette – die

80 Vgl. Hosp (2017), S. 63.

81 Vgl. Hosp (2017), S. 63.

Blockchain.[82] Würde jemand nun versuchen, einen Block in der Kette zu manipulieren, würden sich alle darauffolgenden Transaktionen und Blöcke ebenfalls verändern und das Netzwerk wäre sofort alarmiert und würde den Betrugsversuch erkennen.[83] Darüber hinaus enthält der Header Metadaten wie beispielsweise Zeitstempel und Schwierigkeit, die Nonce sowie den sogenannten Merkle-Root. Über diesen Hash-Baum werden alle im Block befindlichen Transaktionen ebenfalls abgesichert.[84]

Durch das Mining wird die chronologische Reihenfolge und Integrität der Blöcke und somit der Blockchain sichergestellt.[85] Werden alle diese Schritte erfolgreich durchgeführt und das Transaktionsbeispiel von zuvor in einen Block aufgenommen, kann Person X auf die versendete und bestätigte Bitcoin-Adresse durch seine Wallet zugreifen. Hinter der anfänglichen, schematischen und einfachen Darstellung steckt also ein kompliziertes und ausgeklügeltes System, welches ein hohes Maß an Sicherheit und Integrität bietet.

3.2 Konsens-Algorithmen

Neben dem bereits vorgestellten Proof-of-Work gibt es noch die Alternativen Proof-of-Importance und Proof-of-Stake, um sich gemeinsam auf eine identische Version der Blockchain zu einigen (Konsens). Darüber hinaus gibt es durch die Vielzahl an verschiedenen Kryptowährungen ebenfalls eine Vielzahl verschiedener Konsens-Algorithmen. Die meisten sind derzeit noch relativ unbekannt und es ist nicht absehbar, welche sich auch trotz Vorteilen gegenüber anderen auf Dauer durchsetzen werden. Die derzeit relevantesten werden in diesem Unterkapitel betrachtet.

Das Grundprinzip von Proof-of-Work basiert dabei auf der Idee, „dass Miner im Netzwerk nachweisen müssen, dass sie einen gewissen Aufwand aufgebracht haben.“[86] Dieser Mining-Aufwand wurde in Unterkapitel 3.1 im Zusammenhang mit einer Transaktionsbestätigung bereits aufgezeigt. Ohne diesen Algorithmus gäbe es keine neuen Blöcke innerhalb der Blockchain. Vereinfacht gesagt, versuchen die Miner, zu einem

82 Vgl. Stein (2017) (abgerufen am 25. Aug. 2018).

83 Vgl. Hosp (2017), S. 64.

84 Vgl. Lang, Augsten (2017) (abgerufen am 25. Aug. 2018).

85 Vgl. Bitcoin (o. D.) (abgerufen am 27. Aug. 2018).

86 BTC-Echo A (o. D.) (abgerufen am 28. Aug. 2018).

vorgegebenen Output den passenden Input zu finden. Ein wichtiger Teil ist dabei die fehlende Invertierbarkeit, das heißt, dass es nicht möglich ist, anhand des Outputs den Input berechnen zu können, was natürlich deutlich einfacher wäre.[87] Der einzige Weg besteht darin, so lange alle Möglichkeiten durchzuprobieren, bis das Resultat passt. Die Chancen für den Miner, die passende Lösung zu finden, steigen mit höherer Rechenleistung an.[88] Und in diesem Wettrennen per Rechenleistung um die richtige Lösung liegt einer der gravierendsten Nachteile des Proof-of-Work-Algorithmus – der enorm hohe Stromverbrauch bei der Erzeugung neuer Blöcke.

Das Konzept Proof-of-Stake (PoS) ist vergleichbar mit einer Aktiengesellschaft – wer mehr Anteile am Unternehmen hält, darf die Entscheidungen treffen. Bei Proof-of-Stake erhöht die Anzahl an Coins der jeweiligen Währung die Chance, einen neuen Block bestätigen zu dürfen. Dieses Prinzip wird Staking genannt. Je mehr Coins in der Wallet und umso länger im Besitz, desto höher ist die Chance.[89] Dabei stellt sich die Frage, inwieweit ein System dezentralisiert bleiben kann, wenn schlussendlich einige mit vielen Coins sehr viel Macht besitzen und diese zementieren können.[90] Dies bildet auch gleichzeitig den größten Nachteil dieser Methode. Reiche werden reicher und zudem gibt es eine Belohnung, wenn die Geldbeträge gehalten beziehungsweise gestaked werden.

Dabei bietet dieses Prinzip auch einige Vorteile. Die Stimmbeteiligung kann sehr einfach errechnet werden, indem der eigene, eingelegte (gestakte) Geldbetrag durch den gesamten eingelegten Geldbetrag dividiert wird. Wenn ich beispielsweise 1.000 Coins stake und der Gesamtbetrag der Gemeinschaft sich auf 100.000 beläuft, habe ich ein Prozent der Stimmrechte und erhalte ebenfalls ein Prozent der Belohnungen bei Erzeugung eines neuen Blocks.[91] Zudem wird das Mining von der Rechenleistung entkoppelt, was zu einem deutlich geringeren Energieverbrauch im Vergleich zu Proof-of-Work führt.[92]

---

87 Vgl. BTC-Echo A (o. D.) (abgerufen am 28. Aug. 2018).

88 Vgl. Mago, Gillen (2016), S. 16.

89 Vgl. BTC-Echo B (o. D.) (abgerufen am 29. Aug. 2018).

90 Vgl. Koenig (2017), S. 40.

91 Vgl. Hosp (2017), S. 59 f.

92 Vgl. Koenig (2017), S. 39.

Der dritte Konsens-Algorithmus, der in diesem Abschnitt beschrieben wird, nennt sich Proof-of-Importance (PoI, zu Deutsch: Wichtigkeitsnachweis). Dies ist aktuell eine wenig verbreitete Methode zur Konsensbildung, bietet jedoch Vorteile, die die Relevanz in den kommenden Jahren deutlich erhöhen könnte.[93] Dabei wird das Stimmrecht bei Transaktionen durch die Wichtigkeit eines Teilnehmers bestimmt und nicht durch die Rechenleistung oder die Anzahl der Coins. Je höher die Wichtigkeit, desto höher die Chance, Transaktionen bestätigen und einen neuen Block erzeugen zu dürfen. Dieser Vorgang heißt in diesem Fall Ernten und nicht Minen. Das Problem dabei ist allerdings die Frage, wie sich die Wichtigkeit eines Teilnehmers definiert. Dazu gibt es diverse Ansätze, beispielsweise über die Dauer, die der Teilnehmer Teil des Systems ist, über die Anzahl an mit ihm vernetzten Personen oder über die Anzahl an Transaktionen, da Aktivität belohnt werden soll.[94]

Der große Vorteil, insbesondere gegenüber Proof-of-Stake, ist die Gleichberechtigung. Jeder, egal ob arm oder reich, kann ein hohes Maß an Bedeutung erreichen und wichtiger Teilnehmer des Systems werden.[95] Dies ist auch in Hinblick auf die mögliche, zukünftige Alltagstauglichkeit von Blockchain und Kryptowährungen ein wichtiger Faktor. Die Nachteile dieser noch nicht ganz ausgereiften Methode überwiegen allerdings noch. Neben der Schwierigkeit in der Festlegung der Bewertungskriterien ist es relativ leicht, dieses System durch betrügerisches Vorgehen zu schwächen. Durch das Erstellen von vielen Fake-Teilnehmern, die füreinander abstimmen, kann die Konsensbildung manipuliert werden, falls diese betrügerischen Teilnehmer die Mehrheit der Stimmgewalt erreichen.[96]

3.3 Die unterschiedlichen Arten der Blockchain

Bevor in Unterkapitel 3.4 die kryptografischen Grundlagen näher betrachtet werden, folgt eine Übersicht über unterschiedliche Arten der Blockchain.

Eine private Blockchain wird von einzelnen Institutionen für die eigenen Zwecke verwendet und unterliegt deren Kontrolle. Es handelt sich dabei um ein privates Netzwerk

93 Vgl. Hosp (2017), S. 58.

94 Vgl. Crypto Magazin (o. D.) (abgerufen am 01. Sept. 2018).

95 Vgl. Hosp (2017), S. 59.

96 Vgl. Crypto Magazin (o. D.) (abgerufen am 01. Sept. 2018).

und somit ist diese Blockchain weder öffentlich noch wirklich dezentral.[97] Daher ist diese Art von Blockchain eher kritisch zu sehen, zumal die jeweilige Organisation damit ausschließlich die Nachteile, wie Ressourcenverbrauch oder begrenzte Kapazitäten, zu spüren bekommt, während die Vorteile einer offenen Blockchain verwehrt bleiben. Bekannte Kryptowährungen wie Ether oder auch Bitcoin verwenden eine öffentliche Blockchain. Wird in dieser Arbeit oder auch in der Öffentlichkeit von einer Blockchain gesprochen, ist nahezu ausschließlich die öffentliche und dezentrale Version gemeint.[98] Die Eigenschaften sowie Vor- und Nachteile wurden bereits im einleitenden Kapitel 3 angesprochen.

Sidechains sind Abzweigungen der eigentlichen Blockchain (Mainchain) und mit dieser über eine Schnittstelle verbunden.[99] Sie können neben der Mainchain autonom existieren, dazu ist es allerdings notwendig, dass Tokens von der Mainchain auf die Sidechain transferiert und vorrübergehend gesperrt werden. Dies dient dazu, dass diese Tokens nicht doppelt ausgegeben werden können. Die Sidechain stellt dabei eine Art Blackbox dar, das heißt, dass dort viele unabhängige Transaktionen durchgeführt werden können, ohne dass die eigentliche Blockchain davon etwas mitbekommt. Ist die Transaktion nach kurzer Wartezeit abgeschlossen, findet eine Kommunikation der Bestätigung über die Ketten hinweg statt.[100] Anhand eines Bank-Beispiels lässt sich dies einfacher darstellen: Person A überweist Person B einen gewissen Betrag. Diese Transaktion wird von der Bank festgehalten und ist ähnlich einer Transaktion auf der Mainchain. Hebt Person A den gleichen Betrag nun ab, weiß die Bank erstmal nicht, was mit diesem Geld passiert. Person A gibt Person B daraufhin das Geld in Bar – dies entspricht der Sidechain. Anschließend zahlt Person B den Betrag bei seiner Bank wieder ein. Der Kreis schließt sich und das Geld befindet sich wieder bei der Bank, beziehungsweise auf der Mainchain.

97 Vgl. Glücklich A (2017), S 26.

98 Vgl. Glücklich A (2017), S. 26 f.

99 Vgl. Glücklich A (2017), S. 27.

100 Vgl. BTC-Echo C (o. D.) (abgerufen am 05. Sept. 2018).

Die Sidechain kann zudem durch zusätzliche Funktionen, wie beispielsweise Micropayments und Smart Contracts, beliebig ergänzt werden und sogar einen anderen Konsens-Algorithmus verwenden, als die Mainchain.[101] Das bringt zusätzliche Flexibilität innerhalb des Netzwerkes und die eigentliche Blockchain kann entlastet werden, da Transaktionskapazitäten ausgelagert werden.[102] Insbesondere mit Blick auf die Zukunft wird diese Entlastung immer wichtiger, da das bereits starke Datenwachstum innerhalb der Blockchain noch weiter zunehmen wird. Stand September 2018, ist die Bitcoin-Blockchain bereits über 180 Gigabyte groß.[103] Dies erhöht die Menge an Daten, die in die Wallet heruntergeladen werden müssen. Daher weichen Nutzer vermehrt auf Alternativen wie beispielsweise Electrum aus. Dadurch muss nicht mehr die gesamte Blockchain heruntergeladen, sondern lediglich eine Verbindung zu einem Bitcoin-Knoten hergestellt werden. Je mehr Personen auf diese Alternativen ausweichen, desto gefährdeter ist die Stabilität.[104]

Neben den erwähnten Möglichkeiten, anhand derer eine Sidechain die Blockchain erweitern kann, gibt es zudem die Chance für Entwickler, neue Applikationen oder Funktionen risikolos entwickeln und testen zu können.[105] Diese Testnetzwerke sind bei großen Kryptowährungen, insbesondere in Hinblick auf den Wert der Transaktionen, unerlässlich, um eventuelle Schäden in Milliardenhöhe vermeiden zu können.

Einen für die Wirtschaft spannenden Kompromiss zwischen privater und öffentlicher Blockchain stellt die sogenannte konsortiale Blockchain dar, die auch als semi-private Blockchain bezeichnet wird. Teilnehmende Nutzer benötigen die Zustimmung des Konsortiums. Es ist also nicht möglich, den eigentlichen öffentlichen Grundgedanken der Blockchain zu verfolgen und ohne weiteres beizutreten. Diese administrative Beschränkung erhöht allerdings die Attraktivität für Unternehmen, da selbst bestimmt werden kann, wer auf die Transaktionsdaten Zugriff hat.[106]

---

101 Vgl. Glücklich A (2017), S. 27.

102 Vgl. BTC-Echo C (o. D.) (abgerufen am 05. Sept. 2018).

103 Vgl. Blockchain A (o. D.) (abgerufen am 09. Sept. 2018).

104 Vgl. BTC-Echo C (o. D.) (abgerufen am 09. Sept. 2018).

105 Vgl. Glücklich A (2017), S. 27.

106 Vgl. Peter et al. (2017), S. 20 (abgerufen am 30. Sept. 2018).

Dass sich irgendeine Blockchain-Lösung zu 100 Prozent durchsetzt, ist äußerst unwahrscheinlich. Vollkommende Offenheit ist zu unsicher, zu viele Regeln hingegen lassen die Grenzen zu einer herkömmlichen Datenbank verschwimmen. Insbesondere in Hinblick auf die Nutzung in der Wirtschaft werden sich Zwischenlösungen wie die konsortiale Blockchain durchsetzen.

3.4 Kryptografie

Die Kryptografie ist zentraler Bestandteil der Blockchain-Technologie. Ziel dieses Abschnittes ist es, das kryptografische Verfahren aus Kapitel 3 näher zu erklären. Nur so verdeutlicht sich die Sicherheit vor nachträglichen Manipulationen. Als Beispiel findet erneut die Kryptowährung Bitcoin Anwendung.

Der Begriff Kryptografie hat sich als Teildisziplin der Mathematik etabliert und beschäftigt sich mit Methoden zur Verschlüsselung von Informationen.[107] Das Ziel ist es, Daten, Nachrichten und sensible Informationen zu schützen. Um dies zu gewährleisten, gilt es innerhalb der Kryptografie, fünf Grundsätze zu beachten:[108]

- Vertraulichkeit: Die Nachricht soll so verändert werden, dass sie für Außenstehende völlig unlesbar ist und keinerlei Sinn ergibt. Nur berechtige Personen sollen den Inhalt entschlüsseln und lesen dürfen.
- Authentizität: Die Teilnehmer müssen ihre Identität zweifelsfrei nachweisen können. Der Ursprung der Daten oder der Nachricht muss für den Empfänger nachvollziehbar sein. Der Absender muss somit beweisen, dass die Nachricht tatsächlich von ihm stammt, beispielsweise durch eine digitale Signatur.
- Integrität: Die übermittelten Informationen dürfen nicht unbemerkt verändert werden können. Der Absender muss nachweisen, dass die Informationen vollständig sind und diese so verschlüsseln, dass sie im Kern nicht verändert werden.
- Verbindlichkeit: Für den Empfänger einer Nachricht muss nachweisbar sein, dass diese tatsächlich vom Absender stammt. Dies geht über die Authentizität hinaus, da die Nachricht auch authentisch wäre, wenn der Empfänger sich

[107] Vgl. Beutelspacher, Neumann, Schwarzpaul (2010), S. 1.

[108] Vgl. hierzu und im Folgenden Beutelspacher, Neumann, Schwarzpaul (2010), S. 1 f.

selbst überzeugen kann, dass sie vom Absender stammt, es Dritten gegenüber aber nicht beweisen kann. Die Nachweisbarkeit nimmt hier die zentrale Rolle ein.

- Anonymität: Oft wird von lediglich vier Grundsätzen gesprochen. In der Literatur findet die Anonymität als fünfter Grundsatz aber immer häufiger Anwendung, da oftmals neben der Anonymität des Inhalts der Nachricht auch die Anonymität des Absenders und/oder Empfängers und deren Kommunikation gegeben sein soll.

All diese Grundsätze finden Anwendung in der Blockchain und nehmen wichtige Rollen ein. Das angesprochene Konzept der asymmetrischen Kryptografie, also das Verwenden eines zusammengehörenden Schlüsselpaars, geht auf W. Diffie und M. Hellmann im Jahr 1976 zurück.[109]

Eng mit der Kryptografie verbunden ist die Hashfunktion, welche die eingegebenen Daten unabhängig von deren Länge mittels Verschlüsselung als Zeichenfolge mit fester Länge ausgibt.[110] Zurückführen lässt sich der Begriff auf das englische Wort hash (zu Deutsch: Zerhacken oder zerstreuen). Die Hashfunktion des Bitcoins ist der erwähnte SHA256-Algorithmus.[111] SHA steht dabei als Abkürzung für Secure Hash Algorithm.

Als Beispiel für das Hashing dient die folgende Tabelle. Durch den SHA256-Algorithmus entsteht aus einer beliebigen Nachricht eine Hexadezimalzahl:

Eingabewert	**Ausgabewert SHA256**
Hallo, ich heiße Jan.	db057b9b8ee3e42b0ae87b930e2f5b8de57ef32d924332ee9af15e87bd44d2a8
Hallo, ich heiße Jan!	05eee12caa7b5c124cec4be31ac28520d694e25180e5377876a20cb3e9231ffc

Tab. 1: SHA256-Ausgabewerte

(Quelle: Eigene Darstellung nach Xorbin (o. D.) (abgerufen am 11. Sept. 2018)).

[109] Vgl. Beutelspacher, Neumann, Schwarzpaul (2010), S. 4.

[110] Vgl. Blockchain-Nachrichten (2016) (abgerufen am 11. Sept. 2018).

[111] Vgl. Hosp A (2018), S. 51.

Es lässt sich erkennen, dass eine geringfügige Änderung des Eingabewertes zu einem komplett anderen Hash führt. Die Länge des Ausgabewertes bleibt immer gleich , egal ob ich lediglich meinen Namen eingebe oder einen zweiseitigen Text. Folgende Eigenschaften muss eine kryptografische Hashfunktion erfüllen, um als sicher zu gelten:[112]

- Deterministisch: Unabhängig davon, wie oft ein bestimmter Eingabewert eingegeben wird, muss immer der gleiche Ausgabewert dabei herauskommen.
- Schnelligkeit: Um als effizient zu gelten, muss die Hashfunktion in der Lage sein, einen Hash nach Eingabe schnell ausgeben zu können.
- Kleinste Änderungen verändern den gesamten Hash: Wie aus Tabelle 1 zu entnehmen ist, führen kleine Änderungen zu einem völlig anderen Ausgabewert. Dies ist ebenfalls eine kritische Eigenschaft, da diese zu einer der größten Qualitäten der Blockchain führt – die Unveränderlichkeit.
- Kollisionsresistenz: Dabei wird zwischen schwacher und starker Resistenz unterschieden. Schwach bedeutet, dass es nahezu unmöglich ist, für einen gegebenen Wert einen anderen zu finden, der denselben Ausgabewert erzeugt. Stark hingegen heißt, dass es nahezu unmöglich ist, zwei verschiedene Eingabewerte zu finden, die denselben Ausgabewert erzeugen. Diese beiden Resistenzen erscheinen im ersten Augenblick ähnlich stark. Das sogenannte Geburtstagsparadoxon beweist allerdings, dass diese Annahme falsch ist. Für eine 50-prozentige Wahrscheinlichkeit, dass zwei Personen an demselben Tag Geburtstag haben, werden lediglich 23 Personen in einem Raum benötigt. Intuitiv liegt bei vielen Menschen die Einschätzung der Wahrscheinlichkeit deutlich darunter. Wird hingegen ein bestimmter Tag festgelegt, werden für dieselbe Wahrscheinlich von 50 Prozent schon 183 Personen benötigt. Der Unterschied zwischen starker und schwacher Kollisionsresistenz bei kryptografischen Hashfunktionen verhält sich äquivalent.[113]
- Einwegeigenschaft/Pre-Image-Resistenz: Der Hashwert ist einfach zu berechnen, es darf allerdings mit realistischem Aufwand nicht möglich sein, vom Ausgabewert auf den Eingabewert zu schließen. Bei wenigen Werten ist es durch Ausprobieren recht schnell möglich, den Ausgangswert herauszufinden. Als

[112] Vgl. hierzu und im Folgenden Peters (2017) (abgerufen am 15. Sept. 2018).

[113] Vgl. Wenzel-Benner, Wasserrab (o. D.) (abgerufen am 15. Sept. 2018).

Beispiel das Würfeln eines Würfels – heraus kommt dabei ein Hashwert. Wie finde ich nun die eigentliche Zahl heraus? Dazu müssen lediglich die Hashwerte von den Zahlen eins bis sechs verglichen werden und aufgrund der deterministischen Eigenschaft ist so der Ausgangswert zu bestimmen. Bei dem SHA256-Algorithmus ist ein solches Ausprobieren zweckfrei und die Chance, den Eingabewert so herauszufinden, ist astronomisch gering.

Der Hashwert ist mit einem Fingerabdruck vergleichbar. So wie der Fingerabdruck zu einer bestimmten Person gehört, gehört der Hash zu einem bestimmten Datensatz. Der aktuelle Block hat immer den Hashwert des vorherigen Blocks in seiner Kopfzeile, um die Integrität sicherzustellen. Dadurch gilt die Blockchain als praktisch fälschungssicher. Würde jetzt ein Block innerhalb der Blockchain verändert werden, beispielsweise wird eine Transaktion über einen Bitcoin auf 100 Bitcoins geändert, würde sich der Hash im Header des darauffolgenden Blocks ebenfalls verändern und so weiter. Durch die kryptografischen Eigenschaften würde der Betrug sofort im Netzwerk auffallen und der betroffene Benutzer wird ausgeschlossen. Um nicht aufzufallen, müsste der Proof-of-Work für alle auf den veränderten Block folgenden Blöcke neu erbracht werden und das Netzwerk müsste diese nachträglich geänderte Blockchain akzeptieren. Dies ist nur möglich, wenn die manipulierende Person die veränderten Blöcke schneller erzeugt, als das gesamte Netzwerk neue Blöcke an der tatsächlichen Blockchain einspeist. Da hierfür mehr als die Hälfte der Rechenleistung verfügbar sein müsste, wird dieser Angriff auch als 51%-Angriff bezeichnet.[114]

3.5 Mining

Nach Erklärung der kryptografischen Eigenschaften und Grundsätze schließt sich der Kreis zum anfangs in Kapitel 3 erwähnten Mining. Der SHA256-Algorithmus wird von den Mining-Nodes als Werkzeug verwendet, um Transaktionen zusammenzufassen, deren Richtigkeit zu prüfen und anschließend einen Block zu erzeugen. Dabei geht es auch darum, die Transaktionen für unberechtigte Dritte zu verschleiern.[115] Ohne diesen

[114] Vgl. Thiemann (2017), S. 16.

[115] Vgl. Blockchainwelt D (2018) (abgerufen am 15. Sept. 2018).

Algorithmus wäre ein stabiles Bitcoin-Netzwerk unmöglich. Wie im Unterkapitel 3.1 bereits erwähnt, besteht die Schwierigkeit des Minings darin, die passende Nonce zu finden, um den Hashwert zu berechnen.

Aktuell werden zehn Minuten benötigt, um einen neuen Block zu erzeugen. Wird durch zu viel im Netzwerk befindliche Rechenleistung der Proof-of-Work schneller berechnet, passt sich das Netzwerk dahingehend an und erhöht die Schwierigkeit. Alle 2016 Blöcke findet eine automatische Prüfung des Netzwerks statt, ob die Schwierigkeit angepasst werden muss. Diese 2016 Blöcke brauchen immer ungefähr zwei Wochen, bis sie erzeugt wurden.[116] Die Notwendigkeit dieser Zeitspanne besteht darin, da der Bitcoin auf 21 Millionen Coins beschränkt ist.[117] Ohne zusätzliche Schwierigkeit wären diese relativ schnell gemined. Diese Anpassung kann zudem auch heißen, dass die Schwierigkeit wieder nach unten gesetzt wird, da im Vergleich zur letzten Anpassung die Rechenleistung gesunken ist. Der aktuelle Schwierigkeitswert liegt, Stand 15. Sept. 2018, bei 7.019.199.231.177. Anfang 2017 lag dieser bei knapp über 317.000.000.000 – ein starker Anstieg innerhalb kurzer Zeit.[118] Der Schwierigkeitswert stellt dabei dar, wie viel schwieriger es ist, einen aktuellen Block im Vergleich zu dem ersten Block zu erzeugen. In Bezug auf den aktuellen Wert wird also über 7 Billionen Mal mehr Leistung benötigt, als Satoshi Nakamoto benötigte, um den ersten Block zu erstellen.[119]

Eine wichtige Tatsache ist, dass wie bereits im Transaktionsbeispiel erwähnt, das Finden einer Nonce ein reines Glücksspiel ist. Es gibt keine Möglichkeit, sie zu berechnen. Allerdings ist es möglich, die Chancen zu verbessern, einen neuen Block zu erzeugen, indem die sogenannte Hashrate erhöht wird. Diese Hashrate stellt die Anzahl der Versuche pro Sekunde dar, in der eine Nonce ausprobiert wird. Je höher diese Rate, desto mehr Versuche pro Sekunde.[120] Die Hashrate des gesamten Bitcoin-Netzwerkes hat

116 Vgl. Hosp A (2018), S. 74.

117 Vgl. Honig (2018) (abgerufen am 18. Sept. 2018).

118 Vgl. Blockchain B (o. D.) (abgerufen am 18. Sept. 2018).

119 Vgl. Bitcoinmining (o. D.) (abgerufen am 18. Sept. 2018).

120 Vgl. Hosp A (2018), S. 75.

sich im Zeitraum zwischen April und September 2018 verdoppelt und beträgt derzeit über 50.000.000.000 Gigahashes pro Sekunde (GH/s).[121]

Um diese Hashraten und Werte in die richtige Perspektive zu rücken, folgt ein kleines Beispiel zur besseren Einordnung:[122] Ein Mensch hat umgerechnet eine Hashrate von 0,00003 Hashes pro Sekunde (H/s). Würde dieser Mensch versuchen, manuell zu minen, würde es bedeuten, dass er ungefähr neun bis zehn Stunden braucht, um eine einzige Nonce einzusetzen. Die Wahrscheinlichkeit, einen Block zu finden, kann berechnet werden, indem die eigene Hashrate durch die Hashrate des gesamten Netzwerkes dividiert wird. Ausgehend von diesen Fakten und den Zahlen zuvor, wird schnell deutlich, dass ohne technische Hilfsmittel die Chancen auf erfolgreiches Mining praktisch gleich Null sind.

Die meisten Teilnehmer im dezentralen Bitcoin-Netzwerk sind einfache User, die lediglich Transaktionen tätigen wollen und dafür Informationen an Full Nodes und Miner senden. Full Nodes sind Knotenpunkte, die im Gegensatz zum User die gesamte Blockchain speichern, Informationen überprüfen und weiterleiten. Theoretisch kann jeder User zum Miner werden und Transaktionen verifizieren.[123] Am Anfang des Bitcoin-Booms war es noch möglich, ein paar Grafikkarten zu kaufen und Bitcoins am heimischen Computer zu minen. Dieses System wird als Mining-Rig und der dazugehörige Vorgang als GPU-Mining bezeichnet. GPU steht für Graphics Processing Unit und ist eine gängige Abkürzung für eine Grafikkarte. Diese wurden verwendet, da deren Hash-Berechnungen deutlich effizienter sind, als beispielsweise die Verwendung eines Computer-Prozessors (CPU, Central Processing Unit), die lediglich ein bis drei Millionen Hashes pro Sekunde schaffen. Aktuelle Grafikkarten des Herstellers Radeon haben hingegen eine Hashrate von 30 bis 50 Millionen Hashes pro Sekunde.[124]

Diese Zahlen klingen zwar hoch, sind aber im Vergleich zu den Terahashes des Gesamtnetzwerkes gering. Somit lohnen sich aktuell weder das CPU- noch das GPU-Mining für die Kryptowährung Bitcoin. Dies gilt insbesondere für Länder mit hohen

121 Vgl. Bitcoinwisdom (o. D.) (abgerufen am 18. Sept. 2018).

122 Vgl. Hosp A (2018), S. 75 f.

123 Vgl. Hosp A (2018), S. 61 f.

124 Vgl. Hosp A (2018), S. 76.

Stromkosten.[125] Bei noch unbekannteren Kryptowährungen kann sich das GPU-Mining durchaus noch lohnen, ohne dass die Strom- und Anschaffungskosten die Einnahmen überdecken.[126]

Durch die rasante Entwicklung des Bitcoin-Kurses wurden darüber hinaus Chips speziell für das Mining entwickelt. Diese sogenannten Application Specific Integrated Circuit (ASIC) Chips erfüllen neben dem Mining keine andere Funktion und sind dabei ungefähr 100 Mal effizienter als ein GPU-Chip und verbrauchen siebenmal weniger Strom.[127] Die ASIC-Miner dominieren den Bitcoin-Markt und der Hersteller des bekannten Antminers, einer Hardware basierend auf dem ASIC-Chip, ist inzwischen ein Unternehmen mit Umsätzen in Milliardenhöhe. Um diese Dominanz zu brechen, wird bei Kryptowährungen wie Ether, die auf der zweiten Blockchain-Generation basieren, versucht, ASIC-Mining-resistente Mining-Algorithmen zu entwickeln.[128]

Da sich das GPU- oder CPU-Mining zu Hause für viele Kryptowährungen nicht mehr lohnt, stellt das Cloud-Mining eine Alternative dar. Dort braucht der Miner keine eigene Hardware, sondern mietet sich bei einem Cloud-Mining-Anbieter dessen Hashleistung. Diese Anbieter haben je nach Größe eigene Rechenzentren, die rund um die Uhr in Betrieb sind, und stellen diese Infrastruktur zur Verfügung. Oftmals befinden sich die Rechenzentren in Ländern mit geringen Stromkosten.[129]

125 Vgl. Blockchainwelt B (2018) (abgerufen am 19. Sept. 2018).

126 Vgl. Hosp A (2018), S. 76.

127 Vgl. Blockchainwelt B (2018) (abgerufen am 22. Sept. 2018).

128 Vgl. Hosp A (2018), S. 77.

129 Vgl. Blockchainwelt B (2018) (abgerufen am 22. Sept. 2018).

4 Kryptowährungen

Aufbauend auf der detaillierten Darstellung der Blockchain-Technologie und deren Eigenschaften folgt in diesem Kapitel ein Überblick über Kryptowährungen. Zuvor soll zwischen Coins und Token unterschieden werden, da diese häufig fälschlicherweise synonym verwendet werden. Ein Coin ist allgemein gleichzusetzen mit einer Münze oder einem Zahlungsmittel, während ein Token eine breite Funktionalität beinhaltet. Tokens sind zudem auf einer vorhandenen Blockchain aufgebaut, Coins hingegen sind eigenständige Kryptowährungen.[130]

4.1 Bitcoin (BTC)

Der Bitcoin kann definitiv als Mutter aller Kryptowährungen bezeichnet werden. Viele der knapp 2.000 Kryptowährungen wären ohne den Bitcoin niemals entstanden. Nachfolgend werden die wichtigsten Meilensteine der knapp zehn Jahre alten Kryptowährung kurz aufzeigt:

- 01. Nov. 2008: Eine oder mehrere Personen veröffentlichen per Mail unter dem Pseudonym Satoshi Nakamoto ein Whitepaper mit dem Namen ‚Bitcoin: A Peer-to-Peer Electronic Cash System'.[131] Dies stellt das Gründungsdokument für virtuelle Währungen dar.
- 03. Jan. 2009: Nakamoto selbst schürft den ersten Block der Bitcoin-Blockchain, der als Genesis-Block bezeichnet wird. Zusätzlich entstanden die ersten 50 Bitcoins.[132]
- 12. Jan. 2009: Die erste Transaktion mit Bitcoin-Netzwerk findet statt. Nakamoto sendet zehn Bitcoins an eine Person namens Hal Finney.[133]
- 05. Okt. 2009: Erstmals gibt es einen Umtauschkurs von Bitcoin zu US-Dollar. Dieser beträgt 1.309,03 BTC = 1 US-Dollar.[134]
- 22. Mai 2010: Der erste Kauf per Bitcoin wird getätigt. Über ein Bitcoin-Forum kauft Laszlo Hanyecz zwei Pizzen im Wert von 25 US-Dollar für 10.000 Bitcoins.

130 Vgl. Seitz A (2018) (abgerufen am 13. Okt. 2018).

131 Vgl. für das vollständige Whitepaper Nakamoto (o. D.) (abgerufen am 13. Okt. 2018).

132 Vgl. Hosp A (2018), S. 138.

133 Vgl. CoinMarketCap B (o. D.) (abgerufen am 13. Okt. 2018).

134 Vgl. Fried (o. D.) (abgerufen am 13. Okt. 2018).

Mit dem derzeitigen Bitcoin-Kurs wären diese Bitcoins knapp 63 Millionen US-Dollar wert.[135]

- 17. Dez. 2017: Der Kurs eines einzelnen Bitcoins knackt beinahe die Marke von 20.000 US-Dollar und landet bei einem Höchststand von 19.909,50 US-Dollar.[136]

Zudem wurde die Bitcoin-Blockchain währenddessen mehrfach geforked. Bei einem Fork (zu Deutsch: Gabelung) wird eine Blockchain durch eine Änderung des Protokolls in zwei oder mehrere Stränge aufgeteilt.[137] Prinzipiell ist ein Fork wie eine Weiterentwicklung der bestehenden Software zu verstehen. Ein Nutzer wünscht sich neue Funktionalitäten, kopiert die bestehende Blockchain und modifiziert sie. Sinnvoll ist ein solcher Fork nur, wenn genügend Nutzer der abgezweigten Blockchain vorhanden sind.

Dabei kann zwischen Soft- und Hardfork unterschieden werden. Ein Softfork funktioniert wie ein Update, welches ältere Versionen immer noch akzeptiert. Lediglich die Features des Updates können mit der alten Version nicht genutzt werden.[138] Die Nodes mit verschiedenen Versionen arbeiten weiter im Netzwerk zusammen. Eine Hardfork verursacht hingegen immer einen Split, da das Upgrade nicht kompatibel mit der Vorgängerversion ist. Die Nutzer müssen sich entscheiden, welcher Blockchain sie weiter folgen.[139]

Bei Bitcoin gab es bisher zwei Forks, die von Relevanz sind. Am 07. Oktober 2011 stellte Charlie Lee den Litecoin (LTC) als Alternative zum Bitcoin dar. Die gravierendsten Unterschiede liegen in der Transaktionszeit (alle zweieinhalb Minuten ein neuer Block versus zehn Minuten), der maximalen Anzahl an Coins (84 Millionen Litecoins versus 21 Millionen Bitcoins) und im verwendeten Mining-Algorithmus (Scrypt versus SHA256).[140] Bei diesem Hardfork wurde zwar der Code der Mainchain kopiert, allerdings nicht weitergeführt und es entstand ein neuer Genesisblock.

---

135 Vgl. CoinMarketCap B (o. D.) (abgerufen am 13. Okt. 2018).

136 Vgl. CoinMarketCap B (o. D.) (abgerufen am 13. Okt. 2018).

137 Vgl. Hosp A (2018), S. 110.

138 Vgl. Hosp A (2018), S. 111.

139 Vgl. Hosp A (2018), S. 112.

140 Vgl. Hosp A (2018), S. 114.

Bitcoin Cash (BCH) ist das Resultat eines Bitcoin-Forks vom 01. August 2017. BCH besitzt eine maximale Blockgröße von acht Megabyte, was achtmal mehr Transaktionen ermöglicht, als der klassische Bitcoin. Trotz ähnlicher Merkmale gehen die Visionen der beiden Kryptowährungen stark auseinander. Während der Bitcoin sich weiter als digitale, weltweite Geldreserve etablieren möchte, schlägt BCH eher den Weg Richtung weltweit genutzte Währung ein.[141]

Der klassische Bitcoin lässt sich zudem in kleinere Einheiten unterteilen, was für eine angestrebte Bezahlung in der Praxis unerlässlich ist. Dabei reichen die Einteilungen von einem BTC bis zu 0,0000001 BTC, was einem Satoshi entspricht.[142]

4.2 Alternative Kryptowährungen (Altcoins)

Bereits im Jahr 2011 entstanden aus dem Open-Source-Konzept des Bitcoins die ersten alternativen Kryptowährungen.[143] Definiert werden Altcoins als „jede andere Kryptowährung außer Bitcoin“.[144] Inzwischen gibt es über 2.000 verschiedene Kryptowährungen, die alle ihre eigene Blockchain oder alternative Technologien besitzen.[145] Viele sind aufgrund dessen entstanden, dass sich Bitcoin ausschließlich in eine Richtung entwickelt hat.

4.2.1 Ether (ETH)

Die Kryptowährung der Ethereum-Plattform nennt sich Ether und wird mit ETH abgekürzt. In der Praxis werden Ethereum und Ether oft synonym verwendet, was aber genaugenommen falsch ist.[146] Nachfolgend werden die wichtigen Ereignisse der fünfjährigen Geschichte aufgezeigt:

- 2013: Der auch als Wunderkind bezeichnete, 19-jährige Programmierer Vitalik Buterin veröffentlicht erstmals ein Whitepaper über Ethereum, welches das technische Konzept und die dazugehörige Kryptowährung Ether beschreibt.[147]

---

141 Vgl. Hosp A (2018), S. 144.

142 Vgl. Sixt (2017), S. 108.

143 Vgl. Sixt (2017), S. 111.

144 Hosp A (2018), S. 133.

145 Vgl. CoinMarketCap A (o. D.) (abgerufen am 15.10.2018).

146 Vgl. Glücklich B (2017), S. 5.

147 Vgl. Glücklich B (2017), S. 9.

- 22. Jul. 2014: Die Ethereum Foundation startet einen ICO, wodurch interessierte Investoren sich mit Bitcoins Ether kaufen können. Es wurde insgesamt 60 Millionen Ether an Investoren ausgegeben und etwas mehr als 31.000 Bitcoins eingesammelt, was damals einem Wert von ungefähr 15 Millionen US-Dollar entsprach. Somit lag der Preis für einen Ether umgerechnet bei etwa 30 Cent.[148]
- 30. Jul. 2015: Die Ethereum-Plattform geht live und bietet den Nutzern zum ersten Mal die Möglichkeit von Smart Contracts an.[149]
- April 2016: Mithilfe von Smart Contracts wird auf der Ethereum-Blockchain eine sogenannte Dezentralisierte Autonome Organisation (DAO) realisiert. Dabei handelt es sich um eine autonome und dezentrale Beteiligungsgesellschaft, welche in kürzester Zeit knapp 150 Millionen US-Dollar einspielte.[150]
- 18. Jun. 2016: Unbekannte Hacker entwenden durch eine Lücke in den Smart Contracts aus der DAO 3,6 Millionen Ether – damaliger Wert: über 65 Millionen US-Dollar.[151] Dies führte zu einem Beben innerhalb der Ethereum-Community und schwächte die Stellung des Netzwerkes stark.

Repariert wurde dieser Schaden durch einen Hardfork, selbst durchgeführt und initiiert durch Vitalik Buterin. Er kreierte einen neuen Konsens und veränderte somit die Vergangenheit. Die Ethereum-Blockchain wurde so geforked, als ob der Hack niemals stattgefunden hätte. Dieser Eingriff sorgte für viel Unmut, da eine der zentralen Eigenschaften einer Blockchain eigentlich die Unveränderlichkeit der Reihenfolge und Inhalt der Blöcke ist. Zudem wurde die Dezentralität in Frage gestellt.[152]

Durch seinen Einfluss und mithilfe der Community schaffte es Buterin letztendlich, dass die veränderte Blockchain weiterhin Ethereum hieß, während die ursprüngliche Blockchain unter Ethereum Classic weiterläuft.[153] Inzwischen beträgt der Wert von

148 Vgl. Hosp A (2018), S. 145.

149 Vgl. Hosp A (2018), S. 145.

150 Vgl. Niedermeier (2017) (abgerufen am 15. Okt. 2018).

151 Vgl. Glücklich B (2017), S. 10 f.

152 Vgl. Hosp A (2018), S. 148.

153 Vgl. Glücklich B (2017), S. 11.

Ethereum mehr als das 20-fache von Ethereum Classic.[154] Aber auch wie bei Bitcoin und allen anderen Kryptowährungen ist eine verlässliche Vorhersage der Preisentwicklung nicht möglich und beruht auf Spekulationen. Der Kursverlauf gestaltete sich wie folgt:

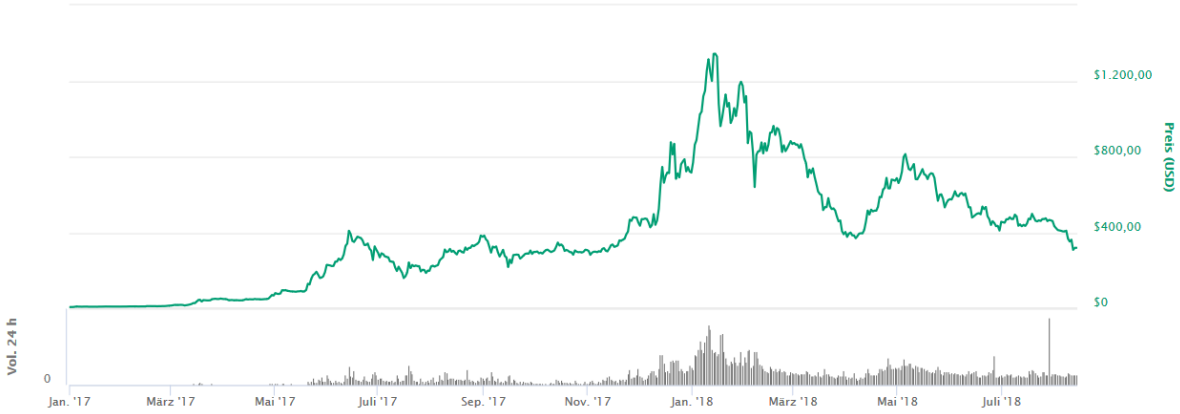

Abb. 5: Kursverlauf Ether vom 01. Jan. 2017 bis 13. Aug. 2018
(Quelle: CoinMarketCap C (o. D.) (abgerufen am 13. Aug. 2018)).

Die für Ethereum zugrundeliegende Blockchain ist die der Bitcoin-Blockchain in weiten Teilen ähnlich. Auch der Mining-Prozess verläuft weitestgehend gleich. Transaktionen werden zu Blöcken zusammengefasst und an den vorherigen Block angehängt. Der Miner, der den gültigen Block per millionenfachem Ausprobieren der Nonce findet, erhält eine Belohnung. Diese beträgt aktuell fünf ETH, zuzüglich der Transaktionsgebühren.[155] Die Zeit für einen neuen Block beträgt beim Bitcoin zehn Minuten, bei Ethereum lediglich 12 bis 15 Sekunden. Durch diese deutlich kürzere Zeitspanne ist die Wahrscheinlichkeit hoch, dass zwei oder mehr Miner gleichzeitig einen gültigen Block finden. Dort setzt sich dann der Block durch, für den als erstes ein Folge-Block gefunden werden kann – der andere Block verwaist hingegen, ähnlich wie bei der Bitcoin-Blockchain. Unterschiedlich ist allerdings die sogenannte Onkel-/Tante-Belohnung, welche bei zwei bis drei Ether liegt. Diese erhält der Miner des verwaisten Blockes, damit seine erbrachte Arbeit in Form von Hardware und Rechenleistung nicht umsonst war.[156]

154 Vgl. CoinMarketCap A (o. D.) (abgerufen am 15. Okt. 2018).

155 Vgl. BTC-Echo E (o. D.) (abgerufen am 09. Okt. 2018).

156 Vgl. Vennekel (2018) (abgerufen am 09. Okt. 2018).

Im Ethereum-Netzwerk werden neben herkömmlichen Transaktionen auch die Smart Contracts durch die Miner prozessiert. Wie bei Bitcoin wird derzeit der Proof-of-Work-Algorithmus zur Konsensfindung verwendet, welcher zukünftig allerdings auf Proof-Of-Stake umgestellt werden soll.[157] Statt des SHA256-Algorithmus findet der sogenannte Ethash Anwendung. Bei diesem Algorithmus wird ebenfalls eine Nonce solange eingesetzt, bis der Hashwert dem vorgegebenen Wert entspricht.[158]

Mithilfe der Smart Contracts ist die Entwicklung sogenannter dezentralisierter Applikationen (dApps) möglich. Diese dApps sind ferner die komplexere Variante der Smart Contracts und lassen sich auch während der Laufzeit auf ihre Korrektheit überprüfen. Eine Software muss folgende vier Kriterien erfüllen, um als dApp zu gelten: Open Source, Blockchain, kryptografisch verschlüsselte Tokens sowie einen eigenen Token-Erzeugungs-Mechanismus. Ethereum erfüllt diese vier Kriterien.[159]

4.2.2 Ripple (XRP)

Ripple (XRP) ist auch bekannt als Bitcoin der Banken und der Beweis dafür, dass auch große Banken sich mit Kryptowährungen und Blockchain in der Praxis beschäftigen. Die Währung des Ripple-Protokolls ist der XRP. Ripple ist ein Enterprise-Projekt, dessen Technologie im Hintergrund läuft und sich so klar von Bitcoin unterscheiden lässt.[160] Das Netzwerk arbeitet mit Banken zusammen und bindet diese sowie weitere Zahlungsdienstleister stark in das Projekt ein. Über das Netzwerk lassen sich jede Art von Werten übertragen und zudem bietet es die Möglichkeit, verschiedene Währungen direkt umzutauschen.[161] Die Transaktionskapazität liegt derzeit bei 1.500 Transaktionen pro Sekunde.[162]

Im Gegensatz zum Bitcoin versteht sich das Ripple-Netzwerk vielmehr als Ergänzung zum klassischen Währungssystem und nicht als Angriff darauf. Der internationale Zahlungsverkehr zwischen Banken soll effizienter und kostengünstiger gestaltet werden.

---

157 Vgl. Vennekel (2018) (abgerufen am 10. Okt. 2018).

158 Vgl. BTC-Echo E (o. D.) (abgerufen am 10. Okt. 2018).

159 Vgl. BTC-Echo D (o. D.) (abgerufen am 10. Okt. 2018).

160 Vgl. BTC-Echo F (o. D.) (abgerufen am 16. Okt. 2018).

161 Vgl. BTC-Echo F (o. D.) (abgerufen am 16. Okt. 2018).

162 Vgl. Grinschuk (2017), S. 40.

Statt Tagen im derzeitigen Korrespondenzbankensystem dauert eine Überweisung im Ripple-Netzwerk zwischen verschiedenen Ländern lediglich Sekunden. Das Netzwerk fungiert als digitales Register, welches alle am Ripple-Protokoll beteiligten Banken jederzeit einsehen können. Es können somit alle Zuschreibungen und Abbuchungen auf den einzelnen Konten transparent nachvollzogen werden. Möchte Bankkunde A aus Australien an Bankkunden B aus Deutschland einen Betrag überweisen, müssen sich im Rahmen der Konsensfindung alle am Ripple-Netzwerk beteiligten Unternehmen und Banken auf eine Transaktion einigen. Dadurch gibt es kein Mining bei Ripple.[163] Der Einigungsvorgang dauert lediglich zwei bis fünf Sekunden und benötigt keine zentrale Verwaltungsstelle.[164] Durch diese Transaktionen werden genaugenommen keine direkten Werte übertragen, sondern lediglich Schuldscheine, auch als IOU (I owe you) bezeichnet. Sogenannte Gateways sorgen im Ripple-Netzwerk dafür, dass bei den Schuldscheinen auch der reale Geldwert übertragen wird.[165] Dabei handelt es sich um kleine, am Netzwerk beteiligte Finanzdienstleister, die die Transaktionen in die gewünschte Fiat- oder auch Kryptowährung umwandeln können.[166]

Die Kryptowährung XRP kann sowohl als Handels- als auch als Wertaufbewahrungsmedium verwendet werden. Sie muss nicht zwangsläufig für Transaktionen eingesetzt werden, sondern dient vielmehr dafür, Angriffe auf das Netzwerk zu verhindern. Durch viele gleichzeitige Transaktionen kann die Netzwerkstabilität gefährdet werden. Im Ripple-Netzwerk verbraucht jede Transaktion die geringe Menge von 0,00001 XRP, sodass ein sogenannter Netzwerkspam schnell zu enormen Kosten führen kann.[167] Wichtig zu wissen ist, dass diese Art von Transaktionsgebühr vernichtet wird und somit die verfügbare Gesamtmenge sinkt. Anfänglich wurden 100 Milliarden XRP generiert und diese Anzahl soll zukünftig nicht weiter erhöht werden. 20 Milliarden XRP behielten die Erfinder selbst, während 80 Milliarden an das Unternehmen Ripple Labs übertragen wurden. Dieses Unternehmen hat sich dazu verpflichtet, über die kommenden

163 Vgl. Grinschuk (2017), S. 40.

164 Vgl. Finanzfluss (o. D.) (abgerufen am 17. Okt. 2018).

165 Vgl. Grinschuk (2017), S. 40.

166 Vgl. BTC-Echo F (o. D.) (abgerufen am 17. Okt. 2018).

167 Vgl. Kryptoszene (o. D.) (abgerufen am 17. Okt. 2018).

vier Jahre 55 Milliarden XRP an Netzwerkteilnehmer auszugeben.[168] Zudem kann XRP als Brückenwährung verwendet werden, falls nicht genügend Liquidität einer bestimmten Währung verfügbar ist.

Der Kursverlauf ist dem der anderen Kryptowährungen sehr ähnlich – aufgrund der hohen Gesamtmenge aber zu einem deutlich geringeren Stückpreis. Nach dem starken Auf- und Abstieg zum Jahreswechsel 2017 auf 2018 hat sich der Kurs inzwischen einigermaßen stabilisiert:

Abb. 6: Kursverlauf Ripple vom 01. Jan. 2017 bis 17. Okt. 2018
(Quelle: CoinMarketCap D (o. D.) (abgerufen am 17. Okt. 2018)).

Abgesehen von dem Kurs gilt es in jedem Fall zu beachten, dass Ripple stark zentralisiert ist und sich fundamental von der Idee des Bitcoins unterscheidet. Das Unternehmen selbst hält derzeit noch weit über 50 Prozent der Anteile, wodurch jederzeit starker Einfluss genommen werden kann. Auch die Mehrzahl an Nodes wird direkt vom Unternehmen Ripple betrieben.[169] Darüber hinaus nutzen die wenigsten der am Ripple-Netzwerk beteiligten Finanzinstitute die Kryptowährung XRP, da der Großteil das sogenannte xCurrent-System verwendet. Dieses System ermöglicht es, internationale Finanztransaktionen in Echtzeit durchzuführen. Zudem sind die Kosten reduziert und Transaktionen nachträglich nicht mehr veränderbar. Allerdings findet die Kryptowährung XRP keine Anwendung.[170]

168 Vgl. Finanzfluss (o. D.) (abgerufen am 17. Okt. 2018).

169 Vgl. Kryptoszene (o. D.) (abgerufen am 17. Okt. 2018).

170 Vgl. Cryptolist A (o. D.) (abgerufen am 17. Okt. 2018).

Im Finanzsektor stellt Ripple ein System mit hohem Zukunftspotenzial dar. Der Widerspruch zum Gedanken von einer dezentralen Plattform, für den die Blockchain-Technologie ursprünglich vorgesehen war, lässt sich nicht wegdiskutieren. Auch der Fakt, dass das Unternehmen Ripple Labs und die Entwickler den Großteil der Coins halten, könnte ein Problem darstellen. Auf der anderen Seite zeugt aber die Zusammenarbeit mit einer Vielzahl an Finanzinstituten, beispielsweise UniCredit, Santander und UBS, von einer Seriosität des Systems.[171] Im Fokus steht ganz klar das System hinter Ripple und nicht die Kryptowährung XRP.

4.2.3 IOTA

Die Idee hinter einer Blockchain ist es, die zentrale Konsensfindung durch einzelne Institutionen zu dezentralisieren. Können Nodes in einer Blockchain jedoch beispielsweise lediglich 100 Transaktionen pro Sekunde bestätigen, so gilt diese Kapazität für die gesamte Blockchain. Ein neuer Ansatz ist es, dass der Konsens gar nicht mehr im gesamten System herrschen muss. IOTA löst dieses Problem durch ein sogenanntes Tangle, welches die Blockchain ersetzt.[172] IOTA wurde im Jahr 2015 von einem renommierten Entwicklerteam gegründet, bestehend aus Entwicklern, Mathematikern und Technologieexperten.[173] Seit Ende 2017 besteht IOTA als gemeinnützige Gesellschaft mit beschränkter Haftung und wird nach deutschem Recht reguliert.[174] Ausgeschrieben steht IOTA für Internet Of Things Alliance (zu Deutsch: Allianz des Internets der Dinge). Dies beschreibt auch gleichzeitig den Hauptgedanken hinter der Technologie – selbstständige Kommunikation unter Maschinen im Rahmen des Internets der Dinge. Schon heute kommunizieren im eigenen Haushalt in Sekundenschnelle das iPad und der iMac miteinander und tauschen Daten aus. IOTA will dies im wirtschaftlichen Kontext und in einem viel höheren Ausmaß leisten.[175]

Das Internet der Dinge und smarte Geräte stellen einen großen Trend in der digitalen Welt dar. Beim Internet der Dinge geht es um eine Vernetzung von Gegenständen mit

171 Vgl. Admiral Markets (o. D.) (abgerufen am 17. Okt. 2018).

172 Vgl. Hosp A (2018), S. 160.

173 Vgl. IOTA Support (o. D.) (abgerufen am 20. Okt. 2018).

174 Vgl. Cryptowolf (2018) (abgerufen am 21. Okt. 2018).

175 Vgl. Cryptowolf (2018) (abgerufen am 21. Okt. 2018).

dem Internet, damit diese selbstständig kommunizieren und Aufgaben erledigen können. Anwendungsbereiche erstrecken sich von privaten Haushalten bis hin zu großen, global agierenden Unternehmen.[176] Dazu gehören auch Smart Homes, in denen beispielsweise der intelligente Thermostat mit dem Smartphone kommuniziert, um so eine gewünschte Temperatur einstellen zu können. Innerhalb der letzten Jahre stieg die Anzahl der mit dem Internet verbundenen Geräte stark an – nach einer Umfrage von Gartner gehen Analysten davon aus, dass im Jahr 2020 das Internet der Dinge mit über 25 Milliarden Geräten zum Alltag gehören wird.[177] IOTA möchte dabei neben der Vernetzung auch gleichzeitig alle finanziellen Aspekte mit dem IOTA-Token (auch als IOTA-Coin bezeichnet) abdecken. Die Gesamtzahl der IOTA-Tokens beträgt 2.779.530.283.277.761, welche in der Einheit MIOTA (eine Million IOTA) an der Kryptobörse gehandelt werden. Auch dessen Kurs hat sich nach einem starken An- und Abstieg zum Jahreswechsel inzwischen stabilisiert:

Abb. 7: Kursverlauf IOTA-Token vom 13. Jun. 2017 bis 21. Okt. 2018

(Quelle: CoinMarketCap E (o. D.) (abgerufen am 21. Okt. 2018)).

Doch warum wird nicht einfach eine beliebige Kryptowährung mit höherer Marktkapitalisierung verwendet? Hier kommen die Vorteile von IOTA zur Geltung. Während sich beispielsweise beim Bitcoin-Netzwerk die Auslastung stark an der Obergrenze bewegt und Transaktionen dadurch langsamer und teurer werden, können bei IOTA deutlich

176 Vgl. Lackes (o. D.) (abgerufen am 21. Okt. 2018).

177 Vgl. Brandt (2014) (abgerufen am 21. Okt. 2018).

mehr Transaktionen pro Sekunde bestätigt werden.[178] Je mehr Teilnehmer im Netzwerk, desto schneller wird dies in seiner Gesamtheit. Das ist ein deutlicher Unterschied zu Bitcoin und Ethereum. Zudem ist IOTA theoretisch unendlich skalierbar und kann die 4.000 Transaktionen pro Sekunde bei Visa deutlich übertreffen.[179] Bitcoin würde bei millionenfachen Micropayments, die im Rahmen des Internets der Dinge pro Sekunde abgewickelt werden, schnell seine Grenzen erreichen.

Aus diesen Gründen setzt IOTA auf den sogenannten Tangle Ledger (zu Deutsch: Gewirr oder Durcheinander), einer Abwandlung der herkömmlichen Blockchain. Optisch lässt sich dies zum besseren Verständnis wie folgt darstellen:

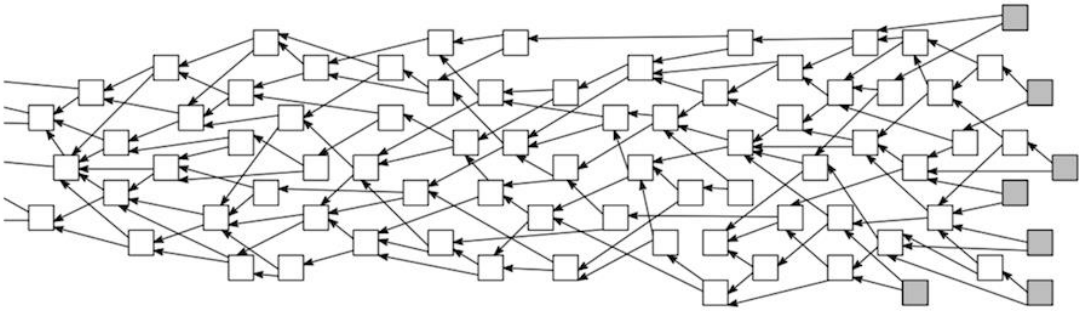

Abb. 8: Tangle-Struktur von IOTA
(Quelle: Popov (2018) (abgerufen am 21. Okt. 2018)).

In diesem Netzwerk gibt es weder Mining-Prozesse noch Blöcke und die Transaktionen sind direkt miteinander verbunden.[180] Somit sind Transaktionen kostenlos. Jedoch müssen die Transaktionen irgendwie bestätigt werden – dies geschieht bei IOTA dadurch, dass mindestens zwei im Vorfeld erfolgreich bestätigte Transaktionen die Voraussetzung sind, um selbst eine Transaktion durchführen zu können. Aus kryptografischer Sicht bildet weiterhin eine Hashfunktion wie aus anderen Blockchains die Grundlage für den Verifikationsprozess.[181]

178 Vgl. Cryptowolf (2018) (abgerufen am 21. Okt. 2018).

179 Vgl. Richter (2017) (abgerufen am 21. Okt. 2018).

180 Vgl. Cryptowolf (2018) (abgerufen am 21. Okt. 2018).

181 Vgl. Cryptolist B (o. D.) (abgerufen am 23. Okt. 2018).

Obwohl sich IOTA noch in einem relativ frühen Entwicklungsstadium befindet, bietet dieses System in der Theorie gewaltige Vorteile, auch in Hinblick auf andere Kryptowährungen. Durch das Tangle-Design ist IOTA beliebig skalierbar und kann theoretisch eine beliebige Zahl an Transaktionen gleichzeitig ausführen.[182] Zu der höheren Anzahl an gleichzeitig durchgeführten Transaktionen kommt gleichzeitig auch eine höhere Geschwindigkeit hinzu. Durch das fehlende Mining gibt es keine Bevorzugung von Transaktionen mit hohen Bearbeitungsgebühren, die der Miner bei erfolgreicher Block-Verifizierung bekommen würde.[183] Die fehlenden Transaktionsgebühren sind insbesondere in Hinblick auf das Internet der Dinge ein kritischer Faktor, da dort millionenfach winzig kleine Transaktionen zwischen Maschinen durchgeführt werden, die sich anderenfalls wirtschaftlich nicht lohnen würden. Das sogenannte Machine to Machine (M2M) Payment, also die autonome und automatische Bezahlung zwischen zwei Maschinen im Internet der Dinge, ließe sich theoretisch auch mit anderen Kryptowährungen wie Bitcoin durchführen – doch dabei wären die Grenzen des Machbaren schnell erreicht. Ausgehend von der endlosen Debatte über die Größe der Blöcke und Skalierbarkeit wird ein Token benötigt, welches winzige Transaktionen in Echtzeit prozessieren kann. Vielen Experten nach kann der IOTA-Token dies leisten, Bitcoin hingegen nicht.[184]

Das Ziel, Rückgrat einer autonomen Ökonomie der Maschinen zu sein, ist ambitioniert. Alle knapp 2,7 Billiarden IOTA-Tokens wurden gegen Bitcoins an Investoren verkauft. Auch große Konzerne zeigen erstes Interesse an IOTA und dem zugehörigen Token. Darunter sind beispielsweise Volkswagen, Bosch und die Deutsche Telekom.[185]

4.3 Handel und Aufbewahrung von Kryptowährungen

Nachdem im Rahmen der Blockchain-Technologie bereits der Transaktionsvorgang anhand des Bitcoins beschrieben wurde, folgt in diesem Unterkapitel ein Überblick darüber, wie Kryptowährungen erworben werden und in welcher Form sie aufbewahrt werden können.

---

182 Vgl. Cryptolist B (o. D.) (abgerufen am 23. Okt. 2018).

183 Vgl. Cryptowolf (2018) (abgerufen am 23. Okt. 2018).

184 Vgl. Bergmann (2016) (abgerufen am 23. Okt. 2018).

185 Vgl. Cryptowolf (2018) (abgerufen am 23. Okt. 2018).

Das Interesse von Investoren an Kryptowährungen stieg in den letzten zwei Jahren stetig an. Neben des Mining-Prozesses, der sich oft nicht mehr rechnet oder sehr aufwändig ist, stehen diverse Plattformen zur Verfügung, die den Erwerb beziehungsweise Handel mit Kryptowährungen ermöglichen.[186] Grundsätzlich lassen sich drei unterschiedliche Handels- und Erwerbsarten unterscheiden, wobei ICOs in Unterkapitel 4.4 nochmal separat betrachtet werden:

- Contracts For Difference (CFD): Diese Methode ist zwar weniger bekannt, hat aber bereits einigen Personen hohe Gewinne gebracht. CFDs stellen einen virtuellen Besitz von Kryptowährungen dar, bei denen auf den Kursverlauf des Coins oder Tokens gewettet wird.[187] Der Handel findet außerhalb der Börse statt und wird per gesetzlich reguliertem Vertrag mit einem Broker geschlossen und durchgeführt. Die Vorteile sind dabei, dass keine Wallet benötigt wird, Käufe und Verkäufe direkt in Euro abgewickelt werden können und der Handel mit CFDs in Europa reguliert ist.[188] Allerdings entsteht dabei eine Abhängigkeit von der Kompetenz des Brokers und das Verlustrisiko ist relativ hoch.
- Exchanges (Börsen): Exchanges erlauben den Kauf, Verkauf und Tausch von einer Vielzahl an Krypto- und Fiat-Währungen.[189] Die inzwischen hohe Anzahl an Exchanges haben teils deutlich unterschiedliche Kursverläufe, sodass sich Vergleiche lohnen. Nach Kauf der Kryptowährung wird der jeweilige Betrag auf die eigene Wallet überwiesen.[190] Bevor der Kauf stattfinden kann, muss sich der jeweilige Käufer im Vorfeld legitimieren, beispielsweise durch Reisepass, Ausweis oder im Idealfall per Video. Dadurch soll Geldwäsche verhindert werden.[191] Abseits von Ether, Bitcoin und Litecoin gestaltet sich der Erwerb von Altcoins an verschiedenen Börsen nicht immer einfach. Oft ist kein direkter Erwerb möglich. Der IOTA-Token zählt derzeit zu den beliebtesten Kryptowährungen, wird aber nur auf wenigen Börsen gehandelt und kann im Euroraum nur über einen

186 Vgl. Bitcoinmag A (o. D.) (abgerufen am 24. Okt. 2018).

187 Vgl. Bitcoinmag A (o. D.) (abgerufen am 24. Okt. 2018).

188 Vgl. Bitcoinmag B (o. D.) (abgerufen am 24. Okt. 2018).

189 Vgl. Hosp A (2018), S. 179.

190 Vgl. Bitcoinmag A (o. D.) (abgerufen am 25. Okt. 2018).

191 Vgl. Hosp A (2018), S. 179.

Umweg erworben werden, indem zuvor beispielsweise Bitcoins gekauft und anschließend getaucht werden müssen.

Somit lässt sich festhalten, dass der Tausch und Handel nicht auch zuletzt aufgrund der Vielzahl an Börsen mit unterschiedlichen Restriktionen abschreckend wirken kann. Für Unternehmen muss im Einzelfall geprüft werden, ob sich ein Kauf oder Handel von Kryptowährungen an einer Börse lohnt. In einem wahrscheinlichen Szenario werden sich zukünftig ein oder mehrere Unternehmen und dessen Kunden auf eine Kryptowährung einigen, mit der bezahlt werden kann.[192] Spannend insbesondere für die Zukunft der Finanzinstitute ist, dass Mitte Juli 2018 in Japan die erste bankgestützte Kryptobörse der Welt eröffnet wurde.[193]

Wurden Kryptowährungen durch einen Handel oder Kauf erworben, spielt in Kombination mit dem Sicherheitsaspekt die richtige Aufbewahrung eine zentrale Rolle. Wie bereits erwähnt, werden die privaten Schlüssel in einer Wallet gespeichert. Die eigentliche Kryptowährung liegt weiterhin auf der Blockchain.[194] Die Wahl der Wallet richtet sich auch nach der Anzahl der Coins und wie lange diese gehalten werden sollen.

Die womöglich sicherste Art der Aufbewahrung ist das sogenannte Paper Wallet*,* also das Schreiben eines privaten Schlüssels auf einem Blatt Papier. Dabei besteht zudem die Möglichkeit, einen QR-Code auszudrucken, um durch Einscannen einen schnellen Zugriff auf die Wallet zu bekommen.[195] Der große Vorteil bei dieser Wallet ist, dass eine einhundertprozentige Sicherheit gegen Hacker besteht. Hacken waren und sind eine der größten Bedrohungen auf dem Markt der Kryptowährungen und haben vielen Besitzern von Kryptowährungen bereits enormen Schaden zugefügt. Nachteilig ist die umständliche Verwendung, daher eignet sich diese Aufbewahrungsmethode insbesondere bei einer hohen Anzahl an Coins, die lange und sicher verwahrt werden sollen.

Des Weiteren gibt es sogenannte Desktop- oder Soft-Wallets*.* Hier wird der private Schlüssel mithilfe einer Software auf dem Computer gespeichert. Dazu wird entweder

192 Vgl. Hosp A (2018), S. 184.

193 Vgl. Giese, T. (2018) (abgerufen am 27. Okt. 2018).

194 Vgl. Hosp A (2018), S. 96.

195 Vgl. Glücklich A (2017), S. 23.

die gesamte Blockchain heruntergeladen, was bei den großen Kryptowährungen schnell einige Hundert Gigabytes werden, oder die sogenannte Simplified Payment Verification (SPV) genutzt. Dabei wird lediglich ein Bruchteil der Blockchain heruntergeladen.[196] Vorteilig ist hier natürlich die Schnelligkeit, da die aufwändige Importarbeit wie bei Paper-Wallets wegfällt, sowie die zusätzlichen Funktionen der Software. Auf der anderen Seite besteht insbesondere bei einer aktiven Internetverbindung die stetige Gefahr durch Hacker, Keylogger und Viren. Daher ist es sinnvoll, den privaten Schlüssel zusätzlich offline als Kopie aufzubewahren.[197]

Um die Vorteile aus Offline- und Online-Aufbewahrung zu kombinieren, begannen Unternehmen sogenannte Hard-Wallets zu entwickeln, auf denen die privaten Schlüssel gespeichert werden. Optisch vergleichbar mit einem USB-Stick, ist ihre Funktionsweise jedoch komplett anders.[198] Sie können nach Einstecken am Computer vom System erst angesprochen werden, wenn am Gerät selbst der richtige PIN eingegeben wird. Somit ist der private Schlüssel offline sicher verwahrt, nach Aktivierung am Computer können dort aber auch die Coins komfortabel versendet und empfangen werden.[199]

4.4 Initial Coin Offering (ICO)

Die ICOs werden noch einmal gesondert betrachtet, da diese in den letzten Jahren innerhalb der Start-Up-Szene einen regelrechten Hype verursacht haben.

Der Begriff ICO wird abgeleitet vom Börsenbegriff IPO, dem Initial Public Offering, also dem Börsengang eines Unternehmens, bei dem Aktien auf dem Kapitalmarkt angeboten werden. Während es bei einem IPO um den Verkauf von Firmenanteilen geht, werden beim ICO Tokens verkauft, die aber ebenfalls Firmenanteilen entsprechen können.[200] In der Regel handelt es sich bei den Tokens aber um die Kryptowährung des

196 Vgl. Glücklich A (2017), S. 23.

197 Vgl. Hosp A (2018), S. 100 f.

198 Vgl. Glücklich A (2017), S. 24 f.

199 Vgl. Hosp A (2018), S. 101.

200 Vgl. Rosenberger (2018), S. 95 f.

Unternehmens, welches das ICO durchgeführt hat und eben dieses erhält im Gegenzug andere Kryptowährungen.[201] Ein bekanntes Beispiel dafür ist die Plattform Ethereum, die im Jahr 2014 im Rahmen ihres ICOs ihre eigene Ether-Kryptowährung gegen Bitcoins verkaufte.

Grundsätzlich lassen sich ICO Tokens in drei unterschiedliche Arten einteilen, die sich auch in ihrer rechtlichen und steuerlichen Behandlung unterscheiden:

- Utility Token: Der Utility-Token erfüllt eine bestimmte Funktion innerhalb des Blockchain-Netzwerkes. Diese häufig verwendete Form schafft einen konkreten Nutzen für den Investor und unterstützt damit direkt die Kaufentscheidung.[202] Dadurch, dass diese Tokens meist als reines Nutzungsrecht einer Leistung ausgestaltet sind, unterliegen diese in der Regel keiner Regulierung. Im Zweifel muss im Einzelfall aber nachgewiesen werden, dass weder Mitspracherecht eingeräumt noch Renditeerwartungen geweckt werden.[203]
- Equity oder Security Token: Dieses Token weist wertpapierähnliche Züge auf und kann mit einer Aktie oder einer Unternehmensbeteiligung verglichen werden. Es wird in das Unternehmen direkt investiert, oft verbunden mit Mitspracherecht und Gewinnbeteiligung.[204] Sie unterliegen grundsätzlich den gleichen Bestimmungen wie klassische Finanzinstrumente und werden daher oft als Wertpapier eingestuft.[205]
- Payment Token: Hierbei handelt es sich um die jeweiligen Kryptowährungen, die ein rein digitales Wertaufbewahrungsmittel darstellen. Die Ausgabe im Rahmen eines ICO ist nicht reguliert, wohl aber der Handel, die Vermittlung und Beratung.[206]

ICOs sind für auf Blockchain basierende Projekte eine beliebte Finanzierungsform geworden und um den anfangs erwähnten Hype wieder aufzugreifen, zeigt folgende Grafik den Investitionsverlauf der letzten Jahre:

---

201 Vgl. Hosp A (2018), S. 149.

202 Vgl. Hahn, Wons (2018), S. 10

203 Vgl. Winheller A (o. D.) (abgerufen am 31. Okt. 2018).

204 Vgl. Hahn, Wons (2018), S. 10.

205 Vgl. Winheller A (o. D.) (abgerufen am 31. Okt. 2018).

206 Vgl. Winheller A (o. D.) (abgerufen am 31. Okt. 2018).

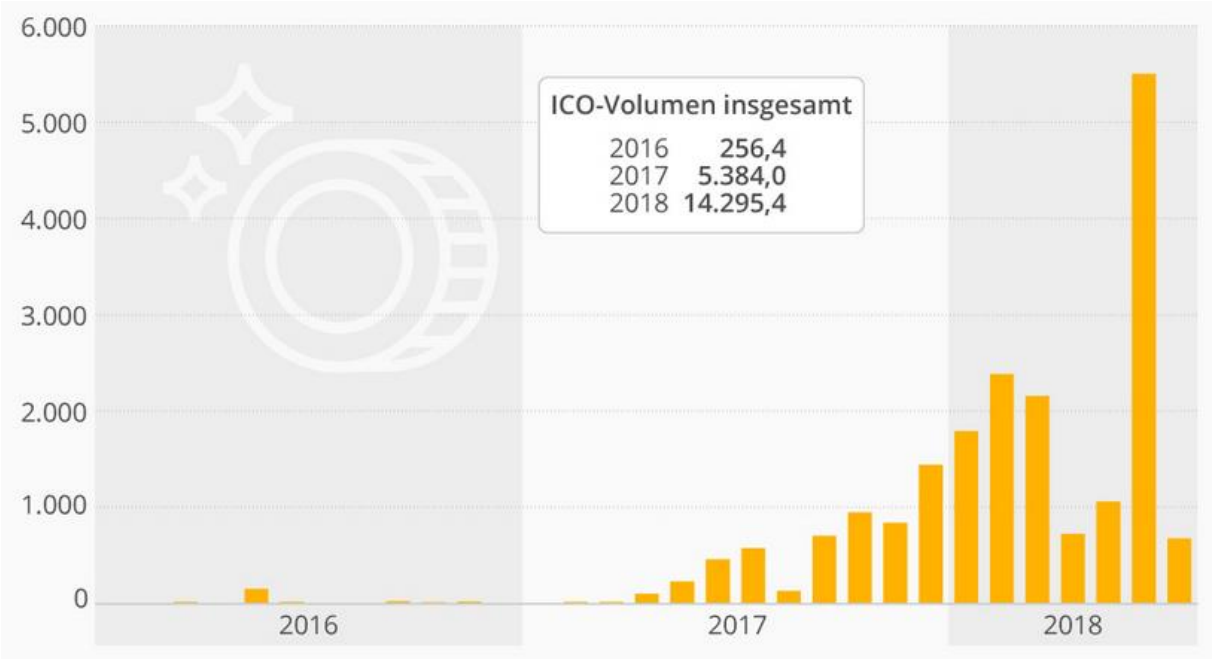

Abb. 9: Höhe der ICO-Investitionen

(Quelle: Brandt (2018) (abgerufen am 29. Okt. 2018)).

Insbesondere Ende 2017 und in der ersten Jahreshälfte von 2018 stiegen die Investitionen stark an. Allein das Unternehmen EOS hat dabei mit einem einjährigen ICO insgesamt knapp 4,1 Milliarden US-Dollar eingenommen.[207] Dieses ICO endete im Juni 2018 und erklärt somit den starken Ausschlag in der oben gezeigten Grafik. Aufgrund des spekulativen Charakters und starken, möglichen Kursschwankungen, wurde von der BaFin im November 2017 eine Verbraucherwarnung herausgegeben.[208] Doch auch diese Warnung hatte vorerst keine negativen Auswirkungen auf das Investitionsvolumen in ICOs, da insbesondere für Tech-Start-Ups die Vorteile anfangs überwiegten.

Erst seit Mitte 2018 nimmt die Entwicklung ab. Grund dafür sind zahlreiche Skandale, in denen Betrüger durch vermeintliche ICOs Geld eingesammelt haben und anschließend abgetaucht sind. Eine fehlende gesetzliche Regulierung führte zu Unsicherheiten, lockte aber auch Geldwäscher und andere Kriminelle an. Zusätzlich stoppten die amerikanische, die europäische und auch die deutsche Börsenaufsicht zahlreiche

[207] Vgl. Diemers et al. (2018), S. 3 (abgerufen am 29. Okt. 2018).

[208] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2017) (abgerufen am 30. Okt. 2018).

ICOs, die in Verbindung mit Betrug standen.[209] Viele der Start-Ups, die besonders an der Finanzierung per ICO interessiert waren, versprachen viel und setzten zu wenig davon um. Es ging einzig und allein darum, in kurzer Zeit möglichst viel Geld einzusammeln. Dadurch wurde die ursprüngliche Idee von ICOs ad absurdum geführt. Es reichten ein paar Schlagwörter wie Blockchain und Kryptowährung, ein kurzes Whitepaper und natürlich ein Button, um Geld investieren zu können. Zudem wurden, wie bereits erwähnt, oft nur Utility-Tokens herausgegeben, was bedeutet, dass der Investor keinerlei Mitspracherecht besitzt und vom Erfolg des Unternehmens und dessen Idee komplett abhängig ist. Vergleichbar ist das mit dem Kauf eines Gutscheines für ein Produkt, welches es noch gar nicht gibt.[210]

Daher kann festgehalten werden, dass der große Hype um ICOs vorbei ist. Heute durchgeführte ICOs haben ganz andere Ansprüche an die Rechtssicherheit, als dies zuvor der Fall war. Ende 2018 werden entsprechend weniger ICOs durchgeführt – die, die aber durchgeführt werden, sind deutlich etablierter und erwachsener.[211] Zudem steht mit dem Security Token Offering (STO) schon eine weitere Form der Unternehmensfinanzierung durch Blockchain in den Startlöchern. Dies wird ICOs zwar nicht in Gänze ersetzen, wohl aber sinnvoll ergänzen. Dabei müssen ausgegebene Tokens durch etwas gestützt sein, beispielsweise Anleihen oder Gewinnbeteiligungen. Der Charakter entspricht somit eher traditionellen Wertpapieren und könnte die Anforderungen der Börsenaufsicht erfüllen.[212] Somit könnten STOs auch für größere Unternehmen interessant sein. Doch auch diese Krypto-Börsengänge müssen erst durch den Gesetzgeber freigegeben werden, um eine tatsächliche, sinnvolle Anwendung in der Praxis darstellen zu können.

[209] Vgl. Bücker (2018) (abgerufen am 31. Okt. 2018).

[210] Vgl. Huber (o. D.) (abgerufen am 31. Okt. 2018).

[211] Vgl. Diemers et al. (2018), S. 9 (abgerufen am 31. Okt. 2018).

[212] Vgl. Bücker (2018) (abgerufen am 31.Okt. 2018).

5 Rechtliche Grundlagen

Kryptowährungen und Blockchain-Technologie haben innerhalb der letzten Jahre stark an Bekanntheit und Relevanz gewonnen. Auch aufgrund dessen konnte der Gesetzgeber bisher kaum rechtliche Rahmenbedingungen dazu schaffen. Zudem haben sich auch vollkommen neue Prozesse entwickelt, die ebenfalls einer Regulierung bedürfen. Da durch das disruptive Potenzial aber auch eine Vielzahl an bestehenden wirtschaftlichen Geschäftsfeldern beeinflusst werden, ist es zwingend notwendig, rechtliche Grundlagen zu schaffen. Die rechtlichen Implikationen ergeben sich teils aus den Charakteristika der Blockchain-Technologie selbst, teils auch aus konkreten Anwendungsfeldern. Es gilt aber auch festzuhalten, dass noch lange nicht alle Implikationen feststellbar sind.[213]

5.1 Datenschutzrecht

Transaktionen zuverlässig, unveränderbar und auf unbestimmte Zeit speichern zu können, ist eine der interessantesten Eigenschaft der Blockchain. In Bezug auf das Datenschutzrecht ist einer der größten Vorteile gleichzeitig die größte Schwäche. Insbesondere durch die im Mai 2018 in Kraft getretene Datenschutzgrundverordnung (DSVGO) entstehen zahlreiche Spannungsfelder. Die DSVGO regelt den Umgang mit personenbezogenen Daten und daher fallen die pseudonymisierten Daten auf der Blockchain eigentlich nicht unter diese Verordnung. Einige Studien belegen aber die Möglichkeit einer Re-Identifizierung von Nutzern der Bitcoin-Blockchain über mit der Blockchain verbundene Dritteinrichtungen, wie beispielsweise Handelsplattformen. Daraus kann schlussendlich auch auf Adressen und Bankverbindungen der Nutzer geschlossen werden.[214] Der Europäische Gerichtshof beschloss im Jahr 2016, dass Daten „dann als personenbezogen gelten, wenn eine verantwortliche Stelle über Mittel verfügt, mit denen die Person durch Zusatzinformationen bestimmt werden kann.“[215] Somit fallen Daten auf Blockchains erst einmal grundsätzlich unter diese Verordnung. Darüber hinaus muss laut Bundesdatenschutzgesetz geklärt sein, welche Stelle oder Person für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten

[213] Vgl. Rauer, Bousonville (2017) (abgerufen am 01. Nov. 2018).

[214] Vgl. Süme, Vogt, Zimprich (2018), S. 28 (abgerufen am 02. Nov. 2018).

[215] Schau (o. D.) (abgerufen am 02. Nov. 2018).

verantwortlich ist.[216] Dies sieht auch die DSVGO vor. Im Konflikt steht dieser Artikel mit dem dezentralen Gedanken der Blockchain, da das System gerade dadurch geprägt ist, dass nicht eine einzelne Person oder Institution die Entscheidungen trifft. Auch hat nicht jeder Nutzer den gleichen Einfluss auf die Blockchain.[217] Hierbei kann auch grundlegend zwischen privater und öffentlicher Blockchain unterschieden werden. Während in einem privaten Netzwerk, beispielsweise zwischen mehreren Unternehmen, verantwortliche Stellen konstruierbar sind, ist es in einem öffentlichen Netzwerk mit den derzeitigen gesetzlichen Regulierungen nicht ohne weiteres möglich und macht eine ohnehin schon unwahrscheinliche Anwendung im öffentlich Bereich in naher Zukunft noch unrealistischer.[218]

Auch reicht die theoretische Rückschließbarkeit vom Pseudonym auf den Klarnamen für viele praktische Anwendungsfälle nicht aus. Dazu zählen Rückabwicklungen im Fall von Schlechtleistungen, Wertpapierhandel oder das Geldwäschegesetz. Darüber hinaus gibt es Anwendungsfälle, in denen die Identität maßgeblich ist, wie beispielsweise Grundbücher, Register und gewerbliche Schutzrechte.[219]

Das wohl größte Konfliktpotenzial liegt in der Kombination mit Artikel 16 und 17 aus der DSVGO – das Recht auf Berichtigung und das Recht auf Löschung der Daten.[220] Bereits im Mai 2014 hat der Europäische Gerichtshof geurteilt, dass Nutzer das Recht haben, ihre personenbezogenen Suchergebnisse aus Suchmaschinen-Indizes entfernen zu lassen, wenn kein öffentlich begründetes Interesse besteht.[221] Artikel 17 DSVGO verallgemeinert dieses Recht auf Vergessen auf europäischer Ebene. Aber eben diese Korrektur und Löschung ist in einer Blockchain nicht möglich. Auch hier werden datenschutzkonforme, öffentliche Blockchains nahezu ausgeschlossen, falls personenbezogene Daten gespeichert werden und zu dem Ergebnis gelangt wird, dass es sich auch tatsächlich um solche handelt. In vielen Anwendungsbereichen

216 Vgl. Süme, Vogt, Zimprich (2018), S. 28 (abgerufen am 02. Nov. 2018).

217 Vgl. Süme, Vogt, Zimprich (2018), S. 28 (abgerufen am 02. Nov. 2018).

218 Vgl. Schau (o. D.) (abgerufen am 02. Nov. 2018).

219 Vgl. PwC (2017) (abgerufen am 02. Nov. 2018).

220 Vgl. Deloitte A (o. D.) (abgerufen am 02. Nov. 2018).

221 Vgl. Deloitte A (o. D.) (abgerufen am 02. Nov. 2018).

scheint eine private oder semi-private Blockchain nach Datenschutzaspekten derzeit die einzig praktikable Lösung.[222]

In ersten Ansätzen, dieses Problem zu umgehen, werden nachträglich editierbare Blockchains diskutiert.[223] Dabei wäre eine vertrauenswürdige Stelle berechtigt, nachträglich Änderungen an der Blockchain vorzunehmen. Widersprüchlich zur eigentlichen Idee der Dezentralität, lässt sich nur so gleichzeitig Editierbarkeit und Aufrechterhaltung der Authentizität gewährleisten. Zudem müssen sich Unternehmen im Einzelfall fragen, wo genau der Mehrwert im Vergleich zu einer herkömmlich kryptografisch abgesicherten Datenspeicherung liegt. Auch das Entfernen von Daten nach einer vorher definierten Zeitspanne stellt eine Option dar – allerdings ist es derzeit noch unklar, ob dies den Ansprüchen der Artikel 16 und 17 DSVGO genügt.[224] Darüber hinaus bestünden die Möglichkeiten, Datenschutzkonformität zu erreichen, indem personenbezogene Daten anderweitig gespeichert werden oder diese Daten bereits verschlüsselt auf der Blockchain gespeichert werden. Durch die im Vorfeld verschlüsselten Daten wäre es nicht mehr möglich, diese auf der Blockchain zu entschlüsseln und es lägen somit nach DSVGO keine personenbezogenen Daten mehr vor. Aber auch diese Ideen laufen dem Sinn einer Blockchain entgegen, zumal einfache Datenintegrität von Unternehmen auch ohne Blockchain gewährleistet werden kann.[225]

Auch wenn in vielen Bereichen mehr Dezentralität wünschenswert wäre, steht das europäische Datenschutzrecht dem vorerst entgegen. Dies verdeutlicht auch das Beispiel von eHealth aus Estland. Dort werden Metadaten der einzelnen Patienten in einer Blockchain gespeichert, sodass jeder Arzt sehen kann, ob er die aktuellen Patientendaten besitzt und wann wer etwas geändert hat. Auch für den Bürger bietet dieses System viele Vorteile wie beispielsweise die Möglichkeit der Prüfung, wer wann welche Daten eingesehen hat. Doch auch hier wurden erste Datenschutzbedenken geäußert, da theoretisch durch die Frequenz der Aktualisierung der Hashwerte Rückschlüsse auf

222 Vgl. Süme, Vogt, Zimprich (2018), S. 28 (abgerufen am 02. Nov. 2018).

223 Vgl. Deloitte A (o. D.) (abgerufen am 02. Nov. 2018).

224 Vgl. Schau (o. D.) (abgerufen am 02. Nov. 2018).

225 Vgl. Schau (o. D.) (abgerufen am 03. Nov. 2018).

die Häufigkeit der Arztbesuche und somit auf den Gesundheitszustand möglich wären.[226]

Beim Thema Datenschutz sind aktuell Gesetzgeber und Unternehmen gefordert. Es muss beachtet werden, dass die DSVGO ohne Bezug zur Blockchain-Technologie entworfen wurde und Bedarf besteht, diese Regulierungen anzupassen. Unternehmen hingegen müssen insbesondere in Hinblick auf das im Artikel 25 DSVGO geforderte Privacy by Design agieren, sodass der Datenschutzaspekt schon bei der Entwicklung berücksichtigt werden muss.[227] Im Rahmen der Risikobewertung ist es erforderlich, die gesetzliche Entwicklung im Auge zu behalten, auch, um möglichen datenschutzrechtlichen Ansprüchen von Nutzern entgegen zu kommen, da Verstöße äußerst empfindliche Strafen mit sich bringen. Daher erscheinen die bereits diskutieren Blockchain-Modifikationen als vorerst beste Lösung.

5.2 Zivilrecht

Das Zivilrecht gilt oft als das im Alltag bedeutendste Rechtsgebiet, da es viele Vorgänge zwischen natürlichen oder juristischen Personen abbildet. Im ersten Schritt stellt sich die Frage, ob Bitcoins oder andere Kryptowährungen rechtlich gesehen wirklich Geld darstellen. Als gesetzlich anerkanntes Zahlungsmittel gilt derzeit nur Bargeld.[228] Nach Privatrecht muss es sich bei Geld um die „für ein bestimmtes Währungsgebiet hoheitlich in Kraft gesetzte Geldverfassung handeln.“[229] Somit sind Kryptowährungen weder gesetzliches Zahlungsmittel noch Geld im rechtlichen Sinne. Zudem scheidet eine Einordnung als Sache mangels Körperlichkeit nach § 90 des Bürgerlichen Gesetzbuches (BGB) ebenfalls aus. Auch eine Einordnung als elektronisches Geld (E-Geld) ist ohne weiteres nicht möglich. Nach dem Zahlungsdiensteaufsichtsgesetz (ZAG) handelt es sich um E-Geld, wenn monetäre Werte elektronisch in Form einer Forderung gegenüber einem Emittenten gespeichert werden. Während die elektronische Form und auch die benötigte Akzeptanz von Dritten erfüllt werden, mangelt es an einem zentralen Emittenten.[230] Dies trifft auf beispielsweise alle Kryptowährungen

226 Vgl. Eibl, Gaedke (Hrsg.) (2017), S. 1035 (abgerufen am 03. Nov. 2018).

227 Vgl. Deloitte A (o. D.) (abgerufen am 03. Nov. 2018).

228 Vgl. Sixt (2017), S. 120.

229 Sixt (2017), S. 120.

230 Vgl. Feil (2018) (abgerufen am 04. Nov. 2018).

zu, die durch Mining erschaffen werden und nicht durch Zahlung eines Geldbetrages. Bei im Vorfeld geschürften Kryptowährungen ist die Rechtslage in Bezug auf E-Geld weiterhin unklar, da diese oft im Gegenzug für andere Kryptowährungen wie Bitcoin erworben werden. Nach der BaFin handelt es sich bei virtuellen Währungen grundsätzlich nicht um E-Geld, außer eine zentrale Stelle tätigt Steuerung und Ausgabe der Einheiten.[231]

Somit sieht das Zivilrecht weder den Ausgleich einer Geldschuld mit Kryptowährungen vor noch können Schadensersatzforderungen damit beglichen werden.[232] Rechtlich gesehen handelt es sich bei der Bezahlung mit Kryptowährungen um ein Tauschgeschäft gemäß § 480 BGB. Einzig, wenn Kryptowährungen nicht nur virtuell existieren, sondern die privaten Schlüssel an einen Datenträger gebunden sind, richtet sich der Erwerb der Coins nach dem Sacheigentum des Datenträgers.[233] Dadurch lassen sich Eigentum und Besitz begründen. Somit kann der private Schlüssel in physischer Form als Eigentum angesehen werden, die auf der Blockchain gespeicherte Kryptowährung hingegen nicht. Bei den Tokens oder Coins als solche handelt es sich im Sinne des § 453 Abs. 1 BGB um sonstige Gegenstände.[234]

Von der Bezahlung mit Kryptowährungen als Gegenleistung muss aus rechtlicher Perspektive der Erwerb von Kryptowährungen mit Fiat-Geld unterschieden werden. Ein Tausch gemäß § 480 BGB scheidet aus, da dieser als Wesen mit sich bringt, dass die Umsetzung ohne Zahlung in Fiat-Währung zu erfolgen hat.[235] Da der Begriff der sonstigen Gegenstände weit gefasst wurde, kann der Vorgang mit dem Kauf einer Software oder virtueller Spielgegenstände verglichen werden. Dieser Kaufvertrag gemäß § 453 I 2. Alt. BGB bietet relative Rechtssicherheit, die sich auf den Kauf von Kryptowährungen übertragen lässt. Als Rechtsfolge besteht nach Zahlung der Fiat-Währung somit ein Anspruch auf die tatsächliche Verschaffung der erworbenen Kryptowährung.[236]

---

231 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (o. D.) (abgerufen am 04. Nov. 2018).

232 Vgl. Feil (2018) (abgerufen am 04. Nov. 2018).

233 Vgl. Sixt (2017), S. 121.

234 Vgl. Kaulartz (o. D.) (abgerufen am 04. Nov. 2018).

235 Vgl. Sixt (2017), S. 123.

236 Vgl. Sixt (2017), S. 123.

Diese Tausch- und Wechselgeschäfte als Ersatz für Bar- oder Buchgeld stellen grundsätzlich erstmal keine erlaubnispflichtige Tätigkeit dar.[237] Erst bei Angeboten gegenüber Dritten bedarf es ab 25 Transaktionen pro Monat einer Erlaubnis, da dann ein gewerbsmäßiger Handel mit Gewinnerzielungsabsicht vorliegt. Große Handelsplattformen und Kryptobörsen, die ihre Tätigkeiten gewerbsmäßig betreiben, brauchen generell eine Erlaubnis. Nicht erlaubnispflichtig hingegen ist das reine Anbieten einer Wallet, da hierbei keine Werte transferiert werden.[238]

Auch bei Haftungsrisiken ist derzeit noch einiges unklar. Dazu gehört auch das Haftungsrisiko zwischen Wallet-Anbieter und Nutzer. Scheidet leichte Fahrlässigkeit aus, stellt sich bei Ansprüchen gegenüber Hackern, falls diese überhaupt ermittelbar sind, die Frage, ob der Bitcoin oder die Kryptowährung überhaupt vom Schutzbereich des § 823 Abs. 1 BGB erfasst wird. Bei physischen Wallets und deren Beschädigung oder Vernichtung kann eine Verletzung angenommen werden. Bei einem Hack und Diebstahl der Kryptowährung greift der Paragraf nicht, da keine Beschädigung vorliegt. Die privaten Schlüssel sind lediglich mit leeren öffentlichen Schlüssen verbunden. Ein möglicher Ansatz liegt darin, Kryptowährungen im Sinne von § 823 Abs.1 BGB als sonstiges Recht zu schützen.[239]

Rechtlich besonders interessant sind Kryptowährungen und Blockchain in Verbindung mit Verträgen, insbesondere Smart Contracts, da hier Verträge hauptsächlich zwischen autonomen Maschinen geschlossen werden. Kommt es zu einem Vertragsbruch, so werden automatisch entsprechende Maßnahmen eingeleitet. Die Blockchain-Technologie dient dabei weniger der Vertragsanbahnung, sondern vielmehr der Vertragsdokumentation.[240] Es ist bisher noch nicht geklärt, inwiefern technische Applikationen rechtlich bindende Abkommen besiegeln dürfen. Grundsätzlich beinhaltet die Vertragsfreiheit in Deutschland die freie Wahl von Form und Inhalt bei der Vertragsausgestaltung. Dennoch setzt ein gültiger Vertragsabschluss Willenserklärungen voraus, die für beide Seiten verständlich sind. Ob ein normaler Nutzer allerdings den

237 Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (o. D.) (abgerufen am 04. Nov. 2018).

238 Vgl. Feil (2018) (abgerufen am 04. Nov. 2018).

239 Vgl. Seitz B (2018) (abgerufen am 04. Nov. 2018).

240 Vgl. Heckmann, Schmid (2017), S. 22 (abgerufen am 04. Nov. 2018).

Programmiercode eines Smart Contracts versteht, ist fraglich. Somit kann angenommen werden, dass viele Smart Contracts ihre Bestimmung in der Umsetzung der vertraglichen Vereinbarungen finden und weniger im Vertragsabschluss selbst.[241] Bei den meisten Smart Contracts werden Verpflichtungs- und Verfügungsgeschäft zusammenfallen, beispielsweise falls Bedingung x eintritt und Rechtsfolge y ausgelöst wird. Diese Verfügung ist auch automatisch ausgeführt eine gültige Willenserklärung und derjenigen Person zurechenbar, die den Befehl festgelegt hat.[242]

Problematischer wird die Zurechnung, je weiter der Mensch in den Hintergrund tritt.[243] Insbesondere für das Internet der Dinge, in dem Maschinen autonom und automatisch miteinander agieren, stellen Smart Contracts das spannendste Anwendungsfeld der Zukunft dar. Doch wo ist die notwendige, menschliche Willenserklärung, wenn die Waschmaschine autonom Waschpulver bestellt und dieses automatisch ausgeliefert wird? Erste Ansätze sprechen vom Anlegen einer sogenannten elektronischen Person (E-Person) mit eigener Rechtspersönlichkeit oder dem automatischen Zustimmen der natürlichen Person hinter der Maschine.[244]

Generell bleibt aber festzuhalten, dass wenn ein Vertrag gültig abgeschlossen wurde, für alle Parteien die Pflicht besteht, den vertraglich festgelegten Obliegenheiten nachzukommen.[245] Allerdings steht die Haftungslage noch nicht fest, falls Programmierfehler innerhalb der Anwendung auftauchen. Eine Korrektur über das Auslegen falscher Klauseln ist nicht möglich. Zudem kann der Smart Contract weder den wirklichen Willen im Sinne von § 133 BGB ermitteln noch Handlungen anders auslegen.[246] Durch die fehlende Auslegungsmöglichkeit geht die Flexibilität des Rechtsbegriffes verloren, beispielsweise bei einer Schadensersatzzahlung nach einer angemessenen Frist. Leistungsmodalitäten müssen klar definiert werden.[247] Ohne menschliche Wertung und Auslegung besteht die Gefahr, Verträge falsch zu gestalten.

---

241 Vgl. Eatough (2017) (abgerufen am 05. Nov. 2018).

242 Vgl. Heckmann, Schmid (2017), S. 24 (abgerufen am 04. Nov. 2018).

243 Vgl. Heckmann, Schmid (2017), S. 25 (abgerufen am 04. Nov. 2018).

244 Vgl. Heckmann, Schmid (2017), S. 25 (abgerufen am 04. Nov. 2018).

245 Vgl. Eatough (2017) (abgerufen am 05. Nov. 2018).

246 Vgl. Schäfer (o. D.) (abgerufen am 05. Nov. 2018).

247 Vgl. Heckmann, Schmid (2017), S. 26 (abgerufen am 05. Nov. 2018).

Bei fehlerhaften Verträgen ergeben sich zudem weitere juristische Komplikationen. Nach deutschem Recht kann gemäß §§ 119 ff. BGB ein Vertrag wegen Irrtums oder Täuschung angefochten werden. Wenn der eigentliche Wille ein anderer war, als der, der vertraglich festgehalten wurde, steht der Person das Recht zu, dass der Vertrag so betrachtet wird, als hätte es ihn nie gegeben.[248] Die Blockchain-Technologie sieht solche Änderungen nicht vor. Auch auf Gewährleistungsrechte kann nicht einfach verzichtet werden. Ein Ansatz wäre es, für die Rückabwicklung einen neuen Smart Contract aufzusetzen. Ebenso wird diskutiert, im Falle von Fehlern oder Rückabwicklungen neutrale, dritte Personen einzusetzen.[249] Theoretisch müssten alle Eventualitäten mit in den Programmcode aufgenommen werden. Wird ein Blick auf herkömmliche Allgemeine Geschäftsbedingungen (AGB) geworfen, fällt auf, wie viele Eventualitäten berücksichtigt werden müssen und wie hoch der entsprechende Programmieraufwand ausfallen würde.[250] In Bezug auf die AGB könnten Bedingungen in Smart Contracts so formuliert sein, dass sie der AGB-Kontrolle gemäß §§ 305 ff. BGB unterliegen. Voraussetzung dafür ist nach § 305 Abs. 1 Satz 1 BGB, dass die Klausel vorformuliert ist, das heißt, sie wird aus einem vorprogrammierten Bestand zur Standardisierung verwendet.[251]

Ein weiteres Problem ergibt sich bei Unterschriften und Signaturen sowie bei Verträgen, die die Mitwirkung eines Dritten erfordern. Ob in der Blockchain eine qualifizierte elektronische Signatur verwendet werden kann, hängt von ihrer technischen Ausgestaltung ab.[252] Ab hier ist es dann auch unklar, ob der digitalen Signatur der gleiche Stellenwert wie der eigenhändigen Unterschrift zukommen kann. Schreibt das Gesetz eine bestimmte Vertragsform vor, so lässt sich dieser Vertrag derzeit nicht rechtskonform als Smart Contract abbilden. Ausschlaggebend ist hierbei die Dokumentations- und Warnfunktion, da der Code von Smart Contracts weder direkt angezeigt wird, noch

248 Vgl. Duisberg (2017) (abgerufen am 05. Nov. 2018).

249 Vgl. Schäfer (o. D.) (abgerufen am 05. Nov. 2018).

250 Vgl. Gogniat (2018) (abgerufen am 05. Nov. 2018).

251 Vgl. Heckmann, Schmid (2017), S. 27 (abgerufen am 05. Nov. 2018).

252 Vgl. Heckmann, Schmid (2017), S. 23 (abgerufen am 05. Nov. 2018).

von jedem lesbar ist.[253] Auch bei einer Mitwirkungspflicht eines Dritten ist eine Abwicklung über die Blockchain nicht rechtskonform. Die notarielle Beurkundung nach § 128 BGB erfüllt ebenfalls eine Beratungs- und Aufklärungsfunktion, daher ist nach derzeitiger Rechtslage eine Abwicklung über ausschließlich digitale Transaktionen nicht sinnvoll, obwohl eine Abwicklung ohne Notar als ein häufig verwendetes Beispiel in Verbindung mit Blockchain genannt wird.[254]

Abschließend kann aus rechtlicher Perspektive festgehalten werden, dass Smart Contracts viel Potenzial bieten, aber fast genauso viele offene juristische Fragen aufwerfen. Im rechtlichen Sinne handelt es sich hierbei nicht um Verträge, vielmehr geht es um die automatische Ausführung und Überwachung der Vertragsinhalte. Die Zeit wird zeigen, für welche Sachverhalte sich Smart Contracts in der Praxis durchsetzen. Es darf davon ausgegangen werden, dass bei weitem nicht alle derzeit diskutierten Beispiele eine praktische Umsetzung finden werden.

5.3 Steuerrecht

Wie bereits festgestellt, sind Kryptowährungen kein gesetzliches Zahlungsmittel und auch kein Geld im eigentlichen Sinne. Die Besteuerung ist gesetzlich nicht explizit geregelt. Vielmehr kommen die allgemeinen Steuerregelungen zur Anwendung, was aber wegen der Neuartigkeit der Kryptowährungen als Wirtschaftsgüter nicht immer unproblematisch ist. Während einige Fragen beantwortet wurden, gibt es immer noch eine Vielzahl an Bereichen und Technologien, die steuerrechtlich nicht eindeutig geklärt sind und im Einzelfall Rechtsberatung erfordern.[255] Das Bundesfinanzministerium hat sich erstmals in einem Schreiben vom 27. Februar 2018 zu der Besteuerung von Kryptowährungen geäußert – allerdings nur in Bezug auf die Umsatzsteuer.[256]

Durch die Einstufung der BaFin als Rechnungseinheiten gemäß § 1 Abs. 11 S. 1 Kreditwesengesetz (KWG) stellt der Handel mit Kryptowährungen ein privates Veräuße-

253 Vgl. Hellinger (2016) (abgerufen am 05. Nov. 2018).

254 Vgl. Heckmann, Schmid (2017), S. 24 (abgerufen am 05. Nov. 2018).

255 Vgl. Winheller B (o. D.) (abgerufen am 06. Nov. 2018).

256 Vgl. Bundesministerium der Finanzen (2018) (abgerufen am 06. Nov. 2018).

rungs- oder Spekulationsgeschäft im Sinne des § 23 Abs. 1 Satz 1 Nr. 2 Einkommensteuergesetz (EStG) dar.[257] Dadurch erfolgt eine Betrachtung als immaterielles Wirtschaftsgut.[258] Im Wesentlichen ist interessant, wie die Veräußerung von Kryptowährungen besteuert wird. Dazu zählen sowohl der Kauf von Kryptowährungen gegen Fiat-Geld, als auch der Erwerb von Waren und Dienstleistungen gegen Kryptowährung.[259] In beiden Fällen liegt das angesprochene private Veräußerungsgeschäft vor. Im Hinblick auf mögliche Veräußerungsgewinne ist nun der Anschaffungszeitpunkt der Kryptowährung ausschlaggebend. Liegt der Anschaffungszeitpunkt der Kryptowährung länger als ein Jahr zurück, so ist der Veräußerungsgewinn steuerfrei. Werden Zinsgewinne mit dem Halten von Kryptowährungen erzielt, fallen diese unter die Abgeltungssteuer und gleichzeitig verlängert sich die Spekulationsfrist auf zehn Jahre.[260] Wird die Kryptowährung innerhalb eines Jahres mit Gewinn veräußert, so fällt diese unter die steuerrechtliche Gesetzesgrundlage gemäß § 23 EStG. Wird die in § 23 Abs. 3 Satz 5 EStG festgelegte Freigrenze von 600 Euro nicht überschritten, bleibt der Gewinn steuerfrei. Bei einer Überschreitung der Freigrenze wird ab dem ersten Euro der gesamte Gewinn mit dem persönlichen Steuersatz versteuert.[261] Bei einem sogenannten Fork werden neben der Blockchain-Historie auch die Steuergeschichte und der Anschaffungszeitpunkt übernommen. Daraus folgt, dass beispielsweise jemand, der am 31. Juli 2016 Bitcoins gekauft hat, seine daraus geforkten Bitcoins Cash am 01. August 2017 steuerfrei veräußern kann. Der Fork stellt somit keinen Anschaffungsvorgang im Sinne des Steuerrechts dar.[262]

Gemäß § 23 Abs. 3 Satz 1 EStG ist der Veräußerungsgewinn der Unterschied zwischen Veräußerungspreis einerseits und Anschaffungs- und Werbungskosten andererseits.[263] Bei der Ermittlung der Anschaffungskosten entsteht häufig das Problem, dass Kryptowährungen zu unterschiedlichen Zeitpunkten zu unterschiedlichen Kursen erworben wurden. Zur Vereinfachung findet hier die sogenannte FIFO-Methode (First

257 Vgl. Zitzmann (2017) (abgerufen am 06. Nov. 2018).

258 Vgl. Winheller B (o. D.) (abgerufen am 06. Nov. 2018).

259 Vgl. Winheller B (o. D.) (abgerufen am 06. Nov. 2018).

260 Vgl. Zitzmann (2017) (abgerufen am 06. Nov. 2018).

261 Vgl. Winheller B (o. D.) (abgerufen am 06. Nov. 2018).

262 Vgl. Finanzgeflüster (2017) (abgerufen am 06. Nov. 2018).

263 Vgl. Winheller B (o. D.) (abgerufen am 06. Nov. 2018).

In First Out) Anwendung.[264] Dadurch wird unterstellt, dass die Coins, die zuerst angeschafft wurden, auch die sind, die im Rahmen des privaten Veräußerungsgeschäftes zuerst eingesetzt werden.[265] Wichtig ist in jedem Fall eine detaillierte Dokumentation der Transaktionen, deren Pflicht beim Steuerpflichtigen liegt. Der ermittelte Gewinn ist in Anlage SO der Steuererklärung aufzuführen. Verluste können mit Gewinnen aus dem Vorjahr oder mittels Verlustvortrag verrechnet werden. Gemäß § 23 Abs. 3 Satz 7 EStG darf die Verrechnung allerdings nur mit Gewinnen aus anderen privaten Veräußerungsgeschäften vorgenommen werden.[266]

Gewerblich tätige Unternehmen und Personen können keine privaten Veräußerungsgeschäfte vornehmen. Geschäfte mit Kryptowährungen, die im Besitz der Unternehmung sind, führen in der Regel zu Einkünften aus einem Gewerbebetrieb gemäß § 15 EStG. Eine Mindesthaltedauer für Steuerfreiheit gibt es nicht. Je nach Rechtsform unterliegen die Gewinne dann der Einkommenssteuer oder der Körperschaftssteuer, sowie jeweils der Gewerbesteuer.[267] Für die Gewerbesteuer sieht § 11 Abs. 1 Satz 3 Nr. 1 GewStG allerdings einen Freibetrag von 24.500 Euro vor.[268]

In Bezug auf die Umsatzsteuer hat das Bundesministerium der Finanzen festgelegt, dass es sich beim Tausch von Kryptowährungen in Fiat-Geld und umgekehrt um eine steuerbare sonstige Leistung handelt, die nach § 4 Nr. 8 b Umsatzsteuergesetz (UStG) umsatzsteuerfrei ist.[269] Bei der Verwendung als Entgelt werden in diesem Falle Bitcoins konventionellen (Fremd-)Währungen im Sinne von § 10 Abs. 1 S. 2 UStG gleichgesetzt.[270] Voraussetzung ist ein ausschließlicher Verwendungszweck als Zahlungsmittel, welcher von der Umsatzsteuer befreit.[271] Rechnungen können im Sinne von § 14 Abs. 4 Nr. 7 UStG steuerkonform in Bitcoin ausgestellt werden – allerdings stellt sich hierbei die Herausforderung der Umrechnung, da die Steuer in Euro abzuführen

264 Vgl. Zitzmann (2017) (abgerufen am 06. Nov. 2018).

265 Vgl. Winheller C (o. D.) (abgerufen am 06. Nov. 2018).

266 Vgl. Zitzmann (2017) (abgerufen am 06. Nov. 2018).

267 Vgl. Winheller C (o. D.) (abgerufen am 07. Nov. 2018).

268 Vgl. Winheller B (o. D.) (abgerufen am 07. Nov. 2018).

269 Vgl. Bundesministerium der Finanzen (2018), S. 1 f. (abgerufen am 06. Nov. 2018).

270 Vgl. Pielke (2018), S. 24.

271 Vgl. Bundesministerium der Finanzen (2018), S. 2 (abgerufen am 06. Nov. 2018).

ist.[272] Die jeweiligen Wechselkurse zur Umrechnung müssen schriftlich nachweisbar sein. Bei internationalen Rechnungen bestimmt sich die Höhe der Umsatzsteuer grundsätzlich zu dem Gegenwert der ausländischen Währung, in dem die Leistung erbracht wird und zu dem Zeitpunkt der Leistungsausführung.[273]

Auch bei der Einordnung des Minings in das Steuerrecht gibt es erste Ansätze. Laut Bundesregierung könnten Einkünfte aus privatem Mining sonstige Einkünfte gemäß § 22 Nr. 3 EStG darstellen.[274] Dies scheint derzeit allerdings noch unklar. Zu dieser Einordnung müsste dem Gewinn im Sinne von § 22 Nr. 3 EStG ein Leistungsbezug zugrunde liegen. Die Rechenleistung ist dabei allerdings nur ein Faktor, vieles beruht auf dem Zufallsprinzip. Zudem wird die Leistung gegenüber einem anonymen Netzwerk erbracht und nicht gegenüber einer Person.[275] Unklar bleibt es auch bei den Transaktionsgebühren, die der Miner als Belohnung erhält. Da diese im direkten Bezug zur Validierung der Transaktionen stehen, könnte eine Steuerpflicht gemäß § 22 Nr. 3 EStG begründet sein.[276] Aufgrund des Aufwandes ist die Schwelle vom privaten ins gewerbliche Mining schnell überschritten, wo dann § 15 EStG Anwendung finden würde. Umsatzsteuerrechtlich handelt es sich beim Mining um nicht steuerbare Vorgänge. Es fällt keine Umsatzsteuer an, genauso wenig kann aber für beispielsweise angeschaffte Hardware die Vorsteuer gemäß § 15 Abs. 2 Nr. 1 UStG abgezogen werden.[277]

Spannend ist die steuerrechtliche Behandlung bei der Blockerstellung durch Proof-of-Stake, welches aufgrund des geringen Energieverbrauches insbesondere bei modernen Kryptowährungen verwendet wird. Hierbei sind Einkünfte aufgrund der Referenz zu bereits vorhandenen Einheiten der jeweiligen Kryptowährung nach § 22 Nr. 3 EStG als steuerpflichtig zu qualifizieren. Dazu muss die Freigrenze von 256 Euro gemäß § 22 Nr. 3 Satz 2 EStG überschritten sein und auch die zehnjährige Spekulationsfrist

272 Vgl. Pielke (2018), S. 24.

273 Vgl. Bundesministerium der Finanzen (2018), S. 2 (abgerufen am 06. Nov. 2018).

274 Vgl. Winheller B (o. D.) (abgerufen am 07. Nov. 2018).

275 Vgl. Pielke (2018), S. 16.

276 Vgl. Pielke (2018), S. 16.

277 Vgl. Winheller B (o. D.) (abgerufen am 07. Nov. 2018).

gemäß § 23 Abs. 1 Nr. 2 Satz 4 EStG dürfte greifen und Steuerfreiheit ausschließen.[278] Aus steuerlicher Perspektive ist dies ein Nachteil im Vergleich zu Proof-of-Work-Tokens. Zudem können beim Staking keine gewerblichen Einkünfte nach § 15 EStG vorliegen, da das Merkmal der aktiven, selbstständigen Tätigkeit nicht erfüllt ist.[279]

In Bezug auf ICOs und Steuerrecht ist eine anfängliche Beratung essentiell. Der Erfolg und die Konformität mit rechtlichen Vorgaben hängen von der Vorarbeit ab. Dies geht über die richtige Ausgestaltung der Tokens bis hin zur Form der Gesellschaft. Im Besteuerungsspektrum zwischen Null und 50 Prozent kann sich durch aktive Gestaltung deutlich der unteren Grenze angenähert werden.[280] Insbesondere bei den Tokens muss gleichermaßen Steuerrecht und Aufsichtsrecht beachtet werden. In der Praxis empfiehlt es sich oft, einer Regulierung durch die BaFin zuzustimmen, um nachhaltige Rechtssicherheit zu schaffen.[281] Bitcoins und andere Kryptowährungen, die ausschließlich im Zahlungsverkehr verwendet werden, sind zwar einerseits von der Umsatzsteuer befreit, andererseits werden bei einem ICO oftmals Tokens mit Geschäftsmodellbezug emittiert. Auch hier bedarf es einer rechtlichen Beratung. Fällt bei Verkauf der Tokens doch Umsatzsteuer an, handelt es sich um eine sonstige elektronische Leistung und die Höhe der Besteuerung richtet sich nach den örtlichen Regeln des Verbraucherwohnsitzes. Insbesondere bei Unkenntnis über die Vorschriften im Ausland kann dies einen erheblichen Einfluss auf das emittierende Unternehmen haben.[282]

Die im Unterkapitel 4.4 erwähnten Tokens, die im Rahmen eines ICO ausgegeben werden können, erfahren teilweise auch eine unterschiedliche rechtliche Behandlung. Werden Tokens als Lohn an die Mitarbeiter des emittierenden Unternehmens ausgegeben, können diese unabhängig von der rechtlichen Einordnung Sachlohn darstellen, der gemäß §§ 19, 38 EStG zu versteuern wäre.[283] Für Privatanleger werden die sogenannten Utility-Tokens als Wirtschaftsgut gemäß §§ 22 Nr. 2, 23 Abs. 1 S. 1 Nr. 2 EStG

278 Vgl. Pielke (2018), S. 17.

279 Vgl. Pielke (2018), S. 17

280 Vgl. Winheller D (o. D.) (abgerufen am 07. Nov. 2018).

281 Vgl. Winheller D (o. D.) (abgerufen am 07. Nov. 2018).

282 Vgl. Winheller D (o. D.) (abgerufen am 07. Nov. 2018).

283 Vgl. Pielke (2018), S. 19.

eingestuft, da für den Kaufpreis das jeweils vorgesehene Recht als Gegenleistung erworben wird. Dieses Recht muss tatsächlich verwertbar sein und anschließende Gewinne aus Veräußerung oder Verwertung der Tokens führen zu einem steuerpflichtigen Gewinn.[284] So kann selbst ein bestimmungsmäßiger Einsatz der Tokens zur Steuerpflicht führen. Equity-Tokens werden Wertpapieren oft gleichgestellt und können daher im Gegensatz zu sonstigen Kryptowährungen der Kapitalertragsteuer gemäß § 20 Absatz 1 EStG unterliegen. Ein Veräußerungsgewinn wäre somit pauschal mit 25 Prozent zu versteuern. Insbesondere die Qualifikation als Kapitaleinkunft hängt von der Ausgestaltung des ICOs ab – eine generelle Aussage ist wie bei vielen anderen Rechtsfragen nicht möglich.[285]

Der wichtigste Unterschied ist, ob ein Token einfach nur ein Inhaber-Token ist oder ob es weitere Merkmale hat, wie beispielsweise Gewinnbeteiligung oder Stimmrechte. Diese Eigenschaften, die ein Token im eigentlichen Sinne erst spannend machen, könnten womöglich erst eine Regulierung bewirken.[286]

Abschließend bleibt festzuhalten, dass auch steuerrechtlich noch viele Fragen offen sind und daher aktuell unbedingt einer Rechtsberatung bedürfen. Werden zu einer Fragestellung die Meinungen mehrerer Juristen gelesen, so ergeben sich daraus oftmals unterschiedliche Ergebnisse. Diese offenen Fragestellungen müssen geklärt und Rechtssicherheit hergestellt werden. Das Bundesministerium der Finanzen beschäftigt sich erst seit etwa zwei Jahren ernstzunehmend mit steuerrechtlichen Fragen zu Kryptowährungen und daher kann es theoretisch passieren, dass sich steuerliche Verhältnisse durch neue Regularien schnell verändern. Dazu zählt beispielsweise eine mögliche Finanztransaktionssteuer oder auch eine Erhebung der Kapitalertragssteuer.

5.4 Lizenzrecht

Obwohl der Gesetzgeber in rechtlichen Fragen zu Kryptowährungen oft hinterherhinkt, wurde die Notwendigkeit der Regulierung und Überwachung des Bitcoin-Systems und anderen Kryptowährungen durch die steigende Popularität schnell erkannt. Plattformen, auf denen gewerblich beispielsweise Bitcoins gehandelt werden, brauchen zum

[284] Vgl. Pielke (2018), S. 20.

[285] Vgl. Pielke (2018), S. 20.

[286] Vgl. Bergmann (2017) (abgerufen am 10. Nov. 2018).

Nutzerschutz und zur Vermeidung von Geldwäsche eine Lizenz. Als Betreiber von Finanzdienstleistungen besteht nach §32 des KWG die Pflicht einer Erlaubniseinholung durch die Aufsichtsbehörde.[287] Je nach Vertragsgestaltung, technischer Umsetzung und Geschäftsmodell kann neben unterschiedlichen Tatbeständen des KWG auch das ZAG berührt sein.[288] Damit ein Unternehmen, welches eine solche Plattform betreibt, unter das KWG fällt, reicht es bereits aus, dass die Dienstleistungen deutschen Kunden angeboten werden – ein Sitz in Deutschland ist nicht notwendig.[289] Dazu gilt es festzuhalten, dass Bitcoin-Systeme nicht unter das KWG fallen, weil der Gesetzgeber besonders schnell die Gesetze angepasst hat. Vielmehr liegt es daran, dass insbesondere die deutsche Gesetzgebung relativ weit gefasst ist und Interpretationsspielräume ermöglicht.[290]

Denkbar ist ebenfalls, dass ein Unternehmer mit seiner Plattform Finanzkommissionsgeschäfte gemäß § 1 Abs. 1 S. 2 Nr. 4 KWG anbietet, also im eigenen Namen handelt, während die Auswirkungen des Handelns Dritte betreffen. Auch hier bedarf es gemäß § 32 Abs. 1 KWG einer BaFin-Lizenz.[291] Dies trifft auch bei multilateralen Handelssystemen zu. In diesem Fall findet per Software auf der Plattform ein sogenanntes Matching statt, das heißt, Käufer und Verkäufer werden automatisch zusammengebracht. Den Vertragsparteien bleibt dabei kein Entscheidungsspielraum, da es lediglich um den reinen Kauf oder Verkauf geht.[292]

Generell ist die Grenze zur Erlaubnispflicht oft fließend.[293] Kommen zur reinen Nutzung der Kryptowährung noch weitere Dienstleistungen hinzu, die einen gewissen Beitrag zum Marktgeschehen leisten, ist eine BaFin-Lizenz in der Regel obligatorisch. Ein erlaubnispflichtiger Eigenhandel nach § 1 Abs. 1a Nr. 4 KWG kann bereits bei 20 Transaktionen pro Monat vorliegen, in denen Bitcoins angekauft oder verkauft werden.[294]

---

287 Vgl. Spancken et al. (2016), S. 10 (abgerufen am 10. Nov. 2018).

288 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

289 Vgl. Spancken et al. (2016), S. 10 (abgerufen am 10. Nov. 2018).

290 Vgl. Spancken et al. (2016), S. 10 (abgerufen am 10. Nov. 2018).

291 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

292 Vgl. Hahn, Wons (2018), S. 34.

293 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

294 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

Auch wenn Unternehmen damit werben, regelmäßig Handel mit Kryptowährungen zu treiben, kann dies nach Ansicht der BaFin ausreichen, um von einem Eigenhandel auszugehen.[295] Vor der gleichen Herausforderung stehen gewerbliche Anbieter von Mining-Pools. Neben den steuerrechtlichen Fragen steht auch hier die Frage nach einer Erlaubnispflicht im Raum.[296]

Für Unternehmen ist es von enormer Wichtigkeit, rechtzeitig zu identifizieren, ob die Leistungen unter die Erlaubnispflicht gemäß ZAG oder KWG fallen. Selbst im Fall des fahrlässigen Handelns entsteht eine Strafbarkeit.[297] Neben der Stilllegung des Geschäftsbetriebes besteht auch Gefahr durch zivilrechtliche Ansprüche der Kunden. In der Regel kann sich der Unternehmer nicht hinter einer haftungsbeschränkten Rechtsform wie einer Gesellschaft mit beschränkter Haftung (GmbH) verstecken, sondern haftet bei Tätigkeit ohne nötige BaFin-Lizenz persönlich.[298]

5.5 Ländervergleich aus rechtlicher Perspektive

Viele der bisher angesprochenen rechtlichen Fragen beziehen sich auf Deutschland. Daneben haben sich auch andere Länder mit Kryptowährungen auseinandergesetzt – die Ergebnisse reichen von Verbot über geringe Rahmenbedingungen bis zu Regulierung und Überwachung. Im globalen Handel können fehlende internationale Standards zu erheblichen Akzeptanzproblemen bei Unternehmen führen.

Argentinien ist eines der Länder, welches Bitcoins als Zahlungsmittel am schnellsten akzeptiert hat. Die Regulierungsbehörden halten sich zurück, um Innovationen ihren Lauf zu lassen und um für eine Selbstregulierung zu sorgen.[299] Daher fallen viele staatliche Eingriffe weg. Zudem ist geplant, bis Ende 2019 über 1.600 Bitcoin-Geldautomaten aufzustellen. Die offene Haltung gegenüber Bitcoin wird auch durch die anhaltende Finanzkrise in Argentinien begründet, um so das Vertrauen der Bürger zurückzugewinnen.[300]

---

295 Vgl. Hahn, Wons (2018), S. 31.

296 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

297 Vgl. Winheller E (o. D.) (abgerufen am 10. Nov. 2018).

298 Vgl. Hahn, Wons (2018), S. 31.

299 Vgl. CLLB Rechtsanwälte (o. D.) (abgerufen am 12. Nov. 2018).

300 Vgl. Neumann (2018) (abgerufen am 12. Nov. 2018).

China hingegen stellt ein Land dar, welches den Handel mit Kryptowährungen und ICOs komplett verboten hat. China wird zwar oft als aufstrebendes Land genannt, besitzt allerdings einen der am strengsten regulierten Märkte weltweit.[301] Kryptowährungen dürften somit im internationalen Handel mit China auf absehbare Zeit keine große Rolle spielen. Dabei ist die Form der digitalen Bezahlung in China kein neues Konzept. Eine Vielzahl der Chinesen nutzt Alipay und WeChat, um Einkäufe zu bezahlen. Zuletzt ging aus Patenten hervor, dass die chinesische Zentralbank womöglich eine eigene Digitalwährung plant, allerdings ohne Dezentralität und unter eigener Kontrolle.[302]

In Bezug auf die Europäische Union (EU) wird nicht nur unter den einzelnen Mitgliedsstaaten der Umgang mit Kryptowährungen diskutiert. Auch die EU-Regulierungsbehörden sind um eine länderübergreifende Gesetzgebung bemüht. Dabei wurde bisher hauptsächlich Einigung erzielt, dass stärkere Regulierungen illegalen Aktivitäten vorbeugen und Börsen unter Regulierung gestellt werden sollen.[303] Bereits im April 2018 stimmte das EU-Parlament mit deutlicher Mehrheit für strengere Regulierungen. Dabei standen die vermeintlich fehlende Transparenz sowie Geldwäsche und Steuerhinterziehung im Fokus. Auch die Volatilität des Marktes ist den Finanzministern der Mitgliedsstaaten ein Dorn im Auge. Als mögliche Lösungsansätze wurden im ersten Schritt das bereits angesprochene Know-Your-Customer-Prinzip und die Durchsetzung von Anti-Geldwäsche-Gesetzen diskutiert.[304] Die Betreiber von Wechselstuben und Kryptobörsen werden zukünftig detailliert erfasst und überwacht. Dabei sollen Nutzerdaten erfasst und zentral gespeichert werden. Belege zu Transaktionen müssen generell für fünf bis zehn Jahre nach Beendigung der Geschäftsbeziehung archiviert werden.[305] Im September 2018 trafen sich die Finanzminister der Mitgliedsstaaten erneut. Dabei kristallisierten sich einige Länder heraus, wie beispielsweise Malta und Zypern, die Chancen für ihr Land als Finanzplatz sehen und strenge EU-Regulierungen vermeiden wollen.[306]

---

301 Vgl. CLLB Rechtsanwälte (o. D.) (abgerufen am 12. Nov. 2018).

302 Vgl. Lange A (2018) (abgerufen am 12. Nov. 2018).

303 Vgl. CLLB Rechtsanwälte (o. D.) (abgerufen am 13. Nov. 2018).

304 Vgl. Eberle, A. (2018) (abgerufen am 13. Nov. 2018).

305 Vgl. Krempl (2018) (abgerufen am 13. Nov. 2018).

306 Vgl. Berschens (2018) (abgerufen am 13. Nov. 2018).

Die entscheidende Frage wird lauten, was passiert, wenn in Bezug auf Kryptowährungen nationale und EU-Gesetzgebung miteinander kollidieren. Durch die unterschiedlichen Haltungen der einzelnen Länder sowie durch Sonderregelungen, wie beispielsweise dem Umgang mit Sparkassen in Deutschland, werden einheitliche europäische Regeln werden in der Praxis schwierig umsetzbar sein.[307] Dass Kryptowährungen in der EU verboten werden, erscheint als sehr unwahrscheinlich. Zudem hat der Ausschuss für Wirtschaft und Währung des EU-Parlaments davon bereits abgeraten. In Bezug auf die Blockchain-Technologie unterzeichneten 22 Mitgliedsstaaten im April ein gemeinsames Abkommen zur Forschung, welches auch die Klärung rechtlicher Fragen beinhaltet.[308] Durch die bisher konservative Haltung der deutsche BaFin zu kryptobasierten Sparplänen überlegen erste Unternehmen, eine Lizenz in weniger strengen Ländern wie Malta oder Zypern anzustreben. Durch den EU-Binnenmarkt könnten diese Unternehmen so ihre Sparpläne auch in Deutschland anbieten.[309] Dieser Fall stellt ein gutes Beispiel für den begrenzten Einfluss nationaler Aufsichtsbehörden innerhalb der EU dar.

In Japan wurde der Bitcoin bereits im Jahr 2017 als legales Zahlungsmittel anerkannt und das Land gilt seither als Vorreiter für die Entwicklung von Blockchain und Krypto-Technologien. Gesetzesvorschriften wurden der Entwicklung entsprechend angepasst und dabei wurde auf Verbote weitestgehend verzichtet. Japan ist allerdings äußerst bestrebt, sich gegen die illegalen Aspekte, beispielsweise Geldwäsche, zu schützen.[310] Auch ist Japan bemüht, das Risikomanagement mit gezielten Eingriffen der japanischen Börsenaufsicht zu verbessern. Dies betrifft in erster Linie Kryptobörsen, da durch den größten Krypto-Hack in der Geschichte über eine halbe Milliarde US-Dollar verloren gingen.[311]

Auch in den USA hat der Gesetzgeber den Bedarf der rechtlichen Regulierung erkannt. Der Vorsitzende der Commodity Futures Trading Commission (CFTC) ist ein starker

[307] Vgl. Kröner (2018) (abgerufen am 13. Nov. 2018).

[308] Vgl. Eberle, A. (2018) (abgerufen am 13. Nov. 2018).

[309] Vgl. Kröner (2018) (abgerufen am 13. Nov. 2018).

[310] Vgl. CLLB Rechtsanwälte (o. D.) (abgerufen am 13. Nov. 2018).

[311] Vgl. Eberle, P. (2018) (abgerufen am 13. Nov. 2018).

Fürsprecher von Kryptowährungen, was unter anderem Anfang 2018 zu einer positiven Anhörung im US-Senat führte.[312] Aber auch hier wird eine Regulierung angestrebt, um illegale Aktivitäten zu vermeiden. Zudem dürfen Kryptobörsen nur mit Lizenz betrieben werden und derzeit ist die Aktivität rund um ICOs noch stark durch den Gesetzgeber eingeschränkt. Tokens könnten unter die nationalen Gesetze zum Wertpapierhandel fallen. Werden diese ohne Erlaubnis im Rahmen eines ICO ausgegeben, kann das emittierende Unternehmen durch Verstoß gegen das Wertpapiergesetz haftbar gemacht werden. Unternehmen versuchen dies teilweise zu umgehen, indem die Tokens als Utility-Tokens ausgegeben werden, was aber zu einer rechtlichen Grauzone und großen Unsicherheiten führt.[313]

[312] Vgl. CLLB Rechtsanwälte (o. D.) (abgerufen am 13. Nov. 2018).

[313] Vgl. Bergmann (2017) (abgerufen am 13. Nov. 2018).

6 Risiken von Kryptowährungen und Blockchain

Dieses Kapitel stellt die Risiken und Grenzen von Kryptowährungen und Blockchain dar, die aktuell in diesem Zusammenhang am häufigsten diskutiert werden.

6.1 Akzeptanz und Komplexität

Wie einleitend erwähnt, ist die bisherige Akzeptanz von Kryptowährungen in der breiten Öffentlichkeit noch nicht weit vorangeschritten. Neben häufiger Medienpräsenz durch volatile Kurse wird als einer der Gründe die hohe Komplexität des Systems aufgeführt. Doch auch der Kryptomarkt selbst gestaltet sich äußerst komplex und ist von einer gewissen Unberechenbarkeit geprägt. Aus technischer Sicht sind Visa und Mastercard dabei nicht weniger kompliziert – allerdings stehen hier Finanz- und Aufsichtsbehörden als Vertrauensgeber dahinter und die Strukturen zur Abwicklung sind gegeben.[314] Auch die stetig wachsende Zahl verschiedener Kryptowährungen führt zu weiterer Verunsicherung. Viele dieser Kryptowährungen haben unterschiedliche technische Eigenschaften. Nutzer wissen derzeit nicht, wohin diese Entwicklung geht und wie interessant eine Kryptowährung in sechs Monaten noch ist.[315]

Eine fehlende Standardisierung wirkt sich auch auf den Zugang zu den Kryptomärkten aus. Nach einer Umfrage der Stuttgarter Börsentochter Sowa Labs gilt dieser als zu komplex, langwierig und teuer.[316] Ist der Sprung in den Kryptomarkt erst einmal geschafft, gestaltet sich das derzeitige Handling der privaten Schlüssel alles andere als benutzerfreundlich. Durch falsche Handhabung droht jederzeit der Verlust der Kryptowährungen.[317] Bei Betrugsfällen gibt es keine zentrale Institution, die helfend eingreifen, Konten sperren oder Kontostände wiederherstellen kann.

Der Faktor Vertrauen spielt auch eine grundsätzliche Rolle, insbesondere wenn es um das Thema Finanzen geht. In Unterkapitel 2.3 wurde bereits kurz diskutiert, dass das Vertrauen in die Banken zwar schwindet, es dennoch viele Vorbehalte gegenüber neuen Technologien gibt, die in den Zahlungsverkehr eingreifen. Diese Skepsis ist beispielsweise in Deutschland, ausgehend von 2015 bis Februar 2018, sogar noch

314 Vgl. Sixt (2017), S. 91.

315 Vgl. Kreditkarten (o. D.) (abgerufen am 17. Nov. 2018).

316 Vgl. Heun (2018), S. 144.

317 Vgl. Badertscher (2016) (abgerufen am 17. Nov. 2018).

gestiegen. Konnten sich damals noch 36 Prozent vorstellen, Bitcoin zu nutzen, waren es Anfang 2018 nur noch knapp 20 Prozent.[318] Damit es wirklich ein radikales Umdenken gäbe, müssten die Banken das bisherige Geldsystem innerhalb kürzester Zeit komplett gegen die Wand fahren. Wie in Unterkapitel 2.2 festgestellt, sind besonders in Deutschland generelle Vorbehalte gegenüber digitalen Zahlungen noch vorhanden. Zwar nutzt die Mehrheit bereits Online-Banking – je kleiner die Beträge werden, desto häufiger kommt Bargeld zum Einsatz.[319] Ähnlich verhält es sich in Deutschland auch in Bezug auf Kryptowährungen und das Alter – je älter die Person, desto kritischer werden Bitcoin und andere Kryptowährungen gesehen und desto geringer ist die Bereitschaft zur Investition. Aber auch ohne Relation zum Alter sieht die Mehrheit der Deutschen digitale Währungen weiterhin kritisch. 21 Prozent gaben dabei die Vielzahl an Betrugsfällen sowie eine fehlende Regulierung als Hauptgründe an.[320] Eine flächendeckende Abwicklung mit Kryptowährungen über eine Blockchain stellt derzeit keine Alternative dar.

Auch viele Unternehmen und Institutionen stehen Kryptowährungen noch skeptisch gegenüber. Einerseits fehlt derzeit für massentaugliche Anwendungen die breite Akzeptanz in der Gesellschaft, andererseits profitieren manche Unternehmen von dem derzeitigen System. Warum sollten Unternehmen wie PayPal, Visa oder Mastercard Interesse daran haben, dass möglichst viele Nutzer eine dezentrale Währung zur Abwicklung ihrer Transaktionen verwenden? Dabei würden fehlende Transaktionsgebühren die Gewinne verringern, während sich gleichzeitig die Stellung am Markt verschlechtert.[321] Visa und Mastercard unterscheiden dabei stark zwischen Kryptowährungen und Blockchain. Während sich beide Unternehmen äußerst interessiert an der Blockchain-Technologie zeigen und teilweise Pionierarbeit in ihrer Branche leisten, wenden beide sich zunehmend von Kryptowährungen ab. Erste Exchanges verzichten daher auf die Bezahlung per Kreditkarte.[322] Auch Banken haben kein Interesse daran, als Intermediäre im Zahlungsverkehr abgelöst zu werden. Dabei geht es ebenfalls um

318 Vgl. Business Insider Deutschland (2018) (abgerufen am 17. Nov. 2018).

319 Vgl. Deutsche Bundesbank (2018) (abgerufen am 17. Nov. 2018).

320 Vgl. Hilmes (2018) (abgerufen am 18. Nov. 2018).

321 Vgl. Glücklich A (2017), S. 35.

322 Vgl. Schmidt A (2018) (abgerufen am 18. Nov. 2018).

den Verlust bestehender Geschäftsmodelle, wie beispielsweise der Abwicklung des Zahlungsverkehrs, und den Verlust der Kontrolle und des Einflusses in der Wirtschaft. Zudem ist es nicht im Interesse der Banken, wenn Anleger ihr Geld vermehrt in dezentrale Kryptowährungen investieren.[323]

Aber inzwischen haben auch die Finanzinstitute erkannt, dass das stetige Aufzeigen diverser Bedrohungsszenarien den grundlegenden Trend nicht aufhalten wird und beschäftigen sich zunehmend mit der Technologie. Erste Investmentbanken profitieren bereits von Kryptofonds und die Blockchain-Technologie könnte insbesondere den internationalen Zahlungsverkehr revolutionieren.[324] Dieses Umdenken ist wichtig – zeigt doch eine Studie der International Business Machines Corporation (IBM) auf, dass Banken in der Finanzwelt weiterhin eine wichtige Rolle spielen werden. Diskutiert werden zudem sogenannte Central Bank Digital Currencies (CBDC), also digitales Geld, ausgegeben durch Zentralbanken.[325] Hierfür könnten auch die Vorteile der Blockchain genutzt werden. Am Ende wird aller Voraussicht nach erst eine Kryptowährung breite Akzeptanz finden, die politisch reguliert wird und hinter der eine zentrale Stelle steht.[326]

Zudem werden durch unterschiedliche Studien und Umfragewerte die Unsicherheiten von Unternehmen teilweise noch verstärkt. Die aktuelle Studie ‚Blockchain in Financial Services 2018' von PricewaterhouseCoopers International (PwC) zeigt nach Befragung von 300 Führungskräften aus Bank- und Versicherungswesen auf, dass Blockchain bei vielen zwar stärker in das Bewusstsein rückt, knapp 70 % diese Technologie allerdings nicht in ihre langfristige Unternehmensstrategie aufnehmen.[327] Der Hälfte reicht es, diese Technologie zeitgleich mit Wettbewerbern einzuführen und keine Vorreiterrolle einzunehmen. Knapp 30 Prozent würden sogar warten, bis sich die Blockchain im Markt etabliert hat. Hier klafft somit eine gewaltige Lücke zwischen Erwartungen und Realität. Dementsprechend stimmt die Mehrheit dafür, dass es bis zur Marktreife mindestens noch zehn Jahre dauern wird. Thomas Schönfeld, Blockchain Leader

323 Vgl. Beckmann & Partner CONSULT (2018) (abgerufen am 18. Nov. 2018).

324 Vgl. Meyer (2018) (abgerufen am 18. Nov. 2018).

325 Vgl. Scheider (2018) (abgerufen am 18. Nov. 2018).

326 Vgl. Binder, Geisler, Schmidt (2017) (abgerufen am 18. Nov. 2018).

327 Vgl. PwC B (2018) (abgerufen am 19. Nov. 2018).

Financial Services bei PwC in Deutschland, und auch die Unternehmensberatung Roland Berger rechnen hingegen damit, dass es branchenweite Lösungen per Blockchain bereits in drei bis fünf Jahren geben wird.[328]

In einer weiteren PwC-Studie aus 2018 wurden weltweit 600 Führungskräfte und Experten aus verschiedenen Branchen befragt. Dabei kam heraus, dass 84 Prozent sich aktiv mit der Blockchain-Technologie beschäftigen – 15 Prozent setzen sogar bereits eigene Projekte um.[329] Interessanterweise wurde dort mit großem Abstand die Finanzbranche als Feld mit dem größten Anwendungspotenzial identifiziert. Dies verdeutlicht die Diskrepanz zwischen (berechtigtem) Hype und realer Anwendung und stellt Unternehmen vor eine zwiespältige Situation.

6.2 Skalierbarkeit

Neben fehlender Akzeptanz und steigender Skepsis ist unter anderem auch der Aspekt der Skalierfähigkeit ein Faktor, der eine weite Verbreitung ausbremst. Grundsätzlich geht es bei einer Skala um eine Einteilung von Größenordnungen. Bei der Fähigkeit, diese Größenordnungen anpassen zu können, wird von Skalierbarkeit gesprochen.[330]

Aufgrund der steigenden Anzahl der Nutzer wird die Skalierung von Kryptowährungen zunehmend zu einem Problem.[331] Bei Bitcoin beispielsweise entsteht eine Limitierung durch die maximale Blockgröße, die vor dem sogenannten Segregated Witness (SegWit) bei einem Megabyte lag. Das hatte zur Folge, dass nur eine begrenzte Anzahl an Transaktionen in einen Block geschrieben und bestätigt werden konnten. Durch diese Beschränkung konnten demnach nur drei bis maximal sieben Transaktionen pro Sekunde abgewickelt werden, abhängig von der Größe.[332] So warteten bereits im Mai 2017 knapp 200.000 Transaktionen darauf, zu der Blockchain hinzugefügt zu werden.[333] Dieser Stauraum für Transaktionen wird auch als Mempool bezeichnet. Dieser

328 Vgl. Springer Professional (2018) (abgerufen am 19. Nov. 2018).

329 Vgl. PwC A (2018) (abgerufen am 19. Nov. 2018).

330 Vgl. Horch A (2018) (abgerufen am 19. Nov. 2018).

331 Vgl. Özel (o. D.) (abgerufen am 19. Nov. 2018).

332 Vgl. Sixt (2017), S. 96.

333 Vgl. Glücklich A (2017), S. 40.

Mempool führte wiederum zu längeren Abwicklungszeiten und zu einem Anstieg der Transaktionsgebühren, da Miner für eine bevorzugte Behandlung erhöhte Gebühren verlangen konnten. Je kleiner und weniger werthaltig die Transaktionen sind, desto geringer ist ihre Priorität – das Bitcoin-Netzwerk ist also für Mikrotransaktionen denkbar ungeeignet.[334] Zudem werden Abwicklungszeiten zunehmend zu einem Problem. Im Bitcoin-Netzwerk können für die endgültige Bestätigung einer Zahlung Stunden vergehen, während beispielsweise am Geldautomaten in Sekundenschnelle Rechtsklarheit herrscht.[335]

Auch der SegWit kann keine dauerhafte Abhilfe schaffen, obwohl im Rahmen dieses Soft-Forks die maximale Blockgröße auf zwei Megabyte erhöht wurde.[336] Während das SegWit-Update inzwischen von immer mehr Usern verwendet wird, ermöglicht es zugleich die Implementierung des sogenannten Lightning-Networks. Der große technologische Fortschritt dahinter ist, dass Zahlungen über separate Micropayment-Kanäle ausgeführt werden, wodurch Buchungen an der Blockchain vorbeilaufen. Zwei Nutzer des Netzwerkes können beliebig viele Transkationen untereinander austauschen, ohne dass alle Teilnehmer des Netzwerkes davon erfahren. Dies ist günstiger und schneller, bedarf allerdings einer vertrauenswürdigen Drittpartei. Lediglich der Endbetrag der Transaktionen wird auf der Blockchain gespeichert und bestätigt.[337] Das Lightning-Network ist derzeit allerdings noch nicht fertiggestellt.

Aber auch Ethereum, dessen Blockchain als deutlich weiterentwickelter als die des Bitcoins angesehen wird, leidet unter fehlenden Skalierungsmöglichkeiten. Ethereum schafft zwar mit 20 Transaktionen pro Sekunde mehr als Bitcoin, ausreichend für eine massentaugliche Anwendung ist aber auch diese Anzahl nicht. Zumal im Ethereum-Netzwerk auch Smart Contracts über Transaktionen laufen und bestätigt werden müssen.[338] Da auch hier das Problem erkannt wurde, entwickelt Ethereum derzeit einige Lösungsansätze. Ein Ansatz heißt Plasma, welches dem Lightning-Netzwerk ähnlich

334 Vgl. Horch A (2018) (abgerufen am 19. Nov. 2018).

335 Vgl. Perlaki (2017) (abgerufen am 19. Nov. 2018).

336 Vgl. Glücklich A (2017), S. 40.

337 Vgl. Giese (2017) (abgerufen am 19. Nov. 2018).

338 Vgl. Glücklich A (2017), S. 40.

ist und erlaubt, Transaktionen an der Blockchain vorbei abzuwickeln.[339] Womöglich die Ideallösung des Skalierungsproblems bei Ethereum ist das sogenannte Sharding. Während es sich bei Plasma um eine Off-Chain-Lösung handelt, was bedeutet, dass der Ansatz sich von der eigentlich Blockchain wegbewegt, ist Sharding eine On-Chain-Methode. Sharding teilt die Knotenpunkte der Blockchain in Gruppen ein. Dadurch muss nicht jeder Knoten und jede Transaktion separat bearbeitet werden. Dabei stellt jede Gruppe einen Shard dar, der alle eingehenden Transaktionen simultan bearbeiten kann. Das Ergebnis ist ein starker Anstieg der Transaktionen pro Sekunde.[340]

Wie relevant das Skalierungsproblem für die alltägliche Anwendung ist, verdeutlicht sich bei einem Blick auf die Transaktionen pro Sekunde von PayPal und Visa. PayPal kommt derzeit auf rund 200 Transaktionen pro Sekunde, kann theoretisch in Stoßzeiten sogar 450 Transaktionen pro Sekunde abwickeln. Visa kommt mit dem VisaNet auf aktuell 2.000 bis 4.000 Transaktionen pro Sekunde – theoretisch liegt der Maximalwert bei 54.000.[341] Bei den derzeitigen Werten sind diese Netzwerke nicht einmal ausgelastet, während sich das Bitcoin-Netzwerk am Limit bewegt. Dadurch sind auch, wie bereits angesprochen, die Gebühren gestiegen, wodurch Bitcoin, von den Transaktionsgebühren her betrachtet, vergleichbar mit einem herkömmlichen Banktransfer ist.[342] Dies mag für eine Überweisung großer Beträge vertretbar sein, für den Einsatz im Alltag hingegen sind hohe Transaktionsgebühren nicht akzeptabel.[343]

Die Verringerung der Transaktionsgröße oder die Erhöhung der Blockgröße stellen weitere Ansätze dar, das Skalierungsproblem zu lösen. Doch beides sind keine dauerhaften Lösungen. Die Verringerung der Größe ist nur bis zu einem gewissen Grade möglich, da die gespeicherten Informationen zumindest einen geringen Datenspeicher benötigen.[344] Wird die Blockgröße, also die Speicherkapazität, erhöht, vergrößert sich

339 Vgl. Özel (o. D.) (abgerufen am 20. Nov. 2018).

340 Vgl. Ernst (2018) (abgerufen am 20. Nov. 2018).

341 Vgl. Kreditkarten (o. D.) (abgerufen am 20. Nov. 2018).

342 Vgl. Marshall (2018) (abgerufen am 20. Nov. 2018).

343 Vgl. BlockLAB (2017) (abgerufen am 20. Nov. 2018).

344 Vgl. Hosp B (2018), S. 81.

gleichzeitig auch die Datenmenge, die jeder Teilnehmer herunterladen muss.[345] Derzeit sinkt die Zahl der Full Nodes, also der User, die die gesamte Blockchain herunterladen, im Bitcoin-Netzwerk. Stand November 2018 liegt die Blockchaingröße bei 190 Gigabyte.[346] Eine Erhöhung der Blockgröße oder eine Verringerung des Intervalls würde dementsprechend dafür sorgen, dass immer weniger Teilnehmer die gesamte Blockchain herunterladen und dadurch die Dezentralität des gesamten Systems gefährden.[347] Nur noch Teilnehmer mit hoher Rechenleistung würden über die Blockerstellung entscheiden. Deutlicher wird das Problem mit einem Vergleich mit Visa. Visa verarbeitet ungefähr 500 Mal so viele Transaktionen pro Sekunde wie Bitcoin – dies führt zu 500 Megabyte großen Blöcken, falls das Intervall pro neuem Block bei zehn Minuten bleiben würde. Pro Stunde würde die Bitcoin-Blockchain demnach um drei Gigabyte, pro Tag sogar um 72 Gigabyte wachsen.[348]

Darüber hinaus sind mehrere Hardforks aus dem Skalierungsproblem hervorgegangen. Zwei der bekanntesten wurden bereits im Unterkapitel 4.1 kurz vorgestellt – Litecoin und Bitcoin Cash, wobei Litecoin eher als Softfork mit Eigenschaften eines Hardforks verstanden werden kann.[349] Beide Kryptowährungen sind gemessen an ihrer Gesamtmarktkapitalisierung sehr erfolgreich und befinden sich Stand November 2018 unter den Top Zehn Kryptowährungen nach Börsenwert.[350] Litecoin ermöglicht alle zweieinhalb Minuten durch den sogenannten Scrypt-Algorithmus eine Blockerstellung, also viermal schneller als das Bitcoin-Netzwerk.[351] Bitcoin Cash, selbst aus dem herkömmlichen Bitcoin hervorgegangen, wurde am 15. November 2018 erneut geforked, um die Blockgröße bis auf 128 Megabyte zu erhöhen. Dadurch sollen schnellere Transaktionen gewährleistet und die Skalierbarkeit verbessert werden. Welche der

345 Vgl. Hosp B (2018), S. 81.

346 Vgl. Blockchain A (o. D.) (abgerufen am 20. Nov. 2018).

347 Vgl. Sixt (2017), S. 96.

348 Vgl. Giese, P. (2018) (abgerufen am 20. Nov. 2018).

349 Vgl. Hosp A (2018), S. 111.

350 Vgl. CoinMarketCap A (o. D.) (abgerufen am 20. Nov. 2018).

351 Vgl. Kerscher (2014), S. 101.

beiden daraus entstandenen Protokolle sich am Ende durchsetzen werden, ist bisher nicht geklärt.[352]

Eine Gefahr in den Lösungsansätzen besteht darin, dass es durch die Vielzahl an möglichen Optimierungen gespaltene Meinungen innerhalb der Community gibt. Viele dieser Ansätze gehen auch in unterschiedliche Richtungen. Somit fehlt eine konkrete Zukunftsvision für das Bitcoin-Netzwerk, wie das Problem der Skalierbarkeit nachhaltig gelöst werden kann. In Bezug auf massentaugliche Anwendungen ist IOTA womöglich am weitesten, da weder Blöcke, Transaktionen noch eine Blockchain verwendet werden. Dort stellt die Skalierbarkeit kein Problem dar, da durch das Tangle zunehmende Zahlen an Nutzern das System sogar noch schneller machen.[353]

6.3 Ressourcenverbrauch

Der Ressourcenverbrauch von Kryptowährungen wird, wie die Skalierung, von Beginn an diskutiert und hat inzwischen eine noch höhere mediale Präsenz erreicht. Der hohe Verbrauch ergibt sich aus dem im Unterkapitel 3.5 vorgestellten Mining in Kombination mit dem häufig verwendeten Konsens-Algorithmus Proof-of-Work (siehe Unterkapitel 3.2). Dieser Algorithmus wird im Bitcoin-Netzwerk sowie noch bei Ethereum verwendet.

Eine Blockchain kann nur betrieben werden, wenn die Miner ihre Hardware rund um die Uhr zum Lösen der mathematischen Aufgaben verwenden.[354] Dabei wird die bereits erwähnte Schwierigkeit im Netzwerk entsprechend der stark steigenden Nutzerzahlen angepasst. Gleichzeitig steigt die benötigte Rechenleistung.[355] Anhand der im Unterkapitel 3.5 dargestellten Zahlen kann erahnt werden, wie viele Millionen Euro Stromkosten am Tag vom System verwendet werden. Diese Energie kann als verschwendet angesehen werden, da im Prinzip das Lösen der mathematischen Aufgabe kein weiteres Ziel verfolgt, als einen Konsens im Netzwerk zu schaffen.[356] Einer neuen, in der Zeitschrift Nature Sustainability veröffentlichten Studie nach, wurden alleine für das

[352] Vgl. Misiak (2018) (abgerufen am 20. Nov. 2018).

[353] Vgl. BlockLAB (2017) (abgerufen am 20. Nov. 2018).

[354] Vgl. Glücklich A (2017), S. 41.

[355] Vgl. Rosenberger (2018), S. 121.

[356] Vgl. Hosp B (2018), S. 79.

Bitcoin-Mining bis Mitte 2018 30,1 Milliarden Kilowattstunden Strom verbraucht – zum Vergleich: Dänemark hatte im Jahr 2015 einen Gesamtstromverbrauch von 31,4 Milliarden Kilowattstunden.[357] Die Schätzungen für den Gesamtenergieverbrauch im Jahr 2018 durch Bitcoin liegen bei 73 Milliarden Kilowattstunden.[358] Die gleiche Studie gibt an, dass für die Erzeugung eines neuen Wertes in Höhe von einem US-Dollar von Anfang 2016 bis Mitte 2018 durchschnittlich 4,7 Kilowattstunden (17 Megajoule) aufgewendet werden mussten. Für herkömmlichen Goldabbau im gleichen Zeitraum wurden lediglich 5 Megajoule pro US-Dollar benötigt und auch viele andere Metalle sind deutlich günstiger in ihrer Erzeugung und in ihrem Abbau.[359] Ausgehend von einem Kurs von 6.275 US-Dollar pro Bitcoin (vor dem starken Rückgang Mitte November), liegt der Energiebedarf für die Erzeugung eines Bitcoins bei 29.500 Kilowattstunden. Dies ist genug, um in Deutschland neun Vier-Personen-Haushalte ein Jahr lang zu versorgen.[360]

Im Vergleich dazu verbraucht beispielsweise Visa, trotz einer deutlich höheren Skalierung und Transaktionsabwicklungsrate, nur einen Bruchteil an Energie. Der Energieverbrauch einer einzigen Bitcoin-Transaktion entspricht dem von mehr als 460.000 Transaktionen im Visa-Netzwerk.[361] Visa verarbeitet derzeit mehr als 80 Milliarden Transaktionen pro Jahr.[362] Eine Studie geht davon aus, dass die Bitcoin-Blockchain mehr Strom verbrauchen würde, als heute weltweit erzeugt werden kann, wenn die Hälfte der Bevölkerung von einem Bankkonto auf Bitcoin wechselt.[363]

Diese gravierenden Umweltprobleme wurden bereits erkannt und stehen zurecht dauerhaft in der Kritik. Ein erster Ansatz ist es, Alternativen zum Proof-of-Work-Algorithmus zu finden. Dabei rücken die unter 3.2 vorgestellten Konsens-Algorithmen in den Fokus. Insbesondere beim Proof-of-Stake würde der energieverbrauchende Aspekt

357 Vgl. Tagesspiegel (2018) (abgerufen am 21. Nov. 2018).

358 Vgl. Harms (2018) (abgerufen am 21. Nov. 2018).

359 Vgl. Schrader (2018) (abgerufen am 21. Nov. 2018).

360 Vgl. Harms (2018) (abgerufen am 21. Nov. 2018).

361 Vgl. Frankfurter Allgemeine Zeitung B (2018) (abgerufen am 22. Nov. 2018).

362 Vgl. Sixt (2017), S. 102.

363 Vgl. Glücklich A (2017), S. 41.

des Minings wegfallen, da nicht mehr die Rechenleistung, sondern der Anteil an Tokens der entscheidende Faktor bei der Transaktionsbestätigung ist.[364] Doch abgesehen vom Umweltaspekt, weisen diese und andere Alternativen noch deutliche Defizite gegenüber Proof-of-Work auf, beispielsweise in Sachen Sicherheit und Dezentralität. Zudem hat sich die mit Abstand größte Kryptowährung Bitcoin mehrfach dazu bekannt, den Proof-of-Work-Algorithmus behalten zu wollen.[365] Ethereum hingegen steckt mitten in der Umstellung auf Proof-of-Stake, um das eigene Konzept für die Zukunft zu unterstreichen. Im ersten Schritt entsteht dazu ein Hybridsystem aus Proof-of-Work und Proof-of-Stake.[366]

Etwa die Hälfte aller Bitcoin-Miningfarmen sind in China angesiedelt und werden somit zum Großteil mit Kohlestrom betrieben.[367] Dementsprechend ist der CO2-Ausstoß durch das Mining enorm und wird von Experten für das Jahr 2018 auf die Menge geschätzt, die bei einer Million Transatlantikflügen entsteht.[368] Vielversprechende Ansätze bestehen darin, die verwendete Energie durch veränderte Algorithmen sinnvoll zu nutzen oder das Mining direkt mit nachhaltigen Energieträgern zu betreiben. Eine sinnvolle Verwendung könnte beispielsweise darin bestehen, die zu lösende Rechenaufgabe so zu gestalten, dass komplexe mathematische Fragestellungen zu relevanten wissenschaftlichen Themen gelöst oder DNS-Rekombinations-Berechnungen durchgeführt werden.[369] In Island oder Norwegen gibt es inzwischen Miningfarmen, die zu 100 Prozent durch ökologisch erzeugten Strom betrieben werden. Bitcoins können somit deutlich günstiger und durch nachhaltige Energie erzeugt werden – im nächsten Schritt soll diese Leistung über einen Mining-Pool vielen Nutzern angeboten werden.[370] Zudem gibt es Ansätze, durch modulare Mining-Geräte die Energie zu recyclen und dabei an einer Stelle gesammelt abzugeben.[371]

364 Vgl. BTC-Echo B (o. D.) (abgerufen am 22. Nov. 2018).

365 Vgl. Hosp B (2018), S. 80.

366 Vgl. Perlaki (2017) (abgerufen am 22. Nov. 2018).

367 Vgl. Tagesspiegel (2018) (abgerufen am 22. Nov. 2018).

368 Vgl. Lange B (2018) (abgerufen am 22. Nov. 2018).

369 Vgl. Hosp B (2018), S. 80.

370 Vgl. Obertreis (2018) (abgerufen am 22. Nov. 2018).

371 Vgl. Horch B (2018) (abgerufen am 22. Nov. 2018).

6.4 Volatilität

Verglichen mit der Ressourcenverschwendung stehen Kryptowährungen womöglich nur durch ihre volatilen Kurse noch häufiger in der Kritik. Die Kursverläufe der größten Kryptowährungen wurden bereits im Kapitel 4 kurz aufgezeigt und es wurde festgestellt, dass sich die Kurse vorerst eigentlich wieder stabilisiert haben. Wie volatil aber der gesamte Markt nach wie vor ist, zeigen die Ereignisse vom 15. November 2018. Ausgehend von einem Wert von knapp 6.300 US-Dollar, ist der Bitcoin Stand 22. November 2018 lediglich noch 4.300 US-Dollar wert.[372] Auch viele andere Kryptowährungen haben innerhalb weniger Stunden dramatische Kursverluste erlitten.

Die Volatilität stellt dabei Fluch und Segen zugleich dar. Ein Segen ist sie für alle Spekulanten und Daytrader, denen dadurch hohe Gewinnmargen ermöglicht werden. Fluch hingegen ist sie, wenn es um verlässliche und planbare Zahlungen geht, denn um effizientes Wirtschaften ermöglichen zu können, ist ein stabiler Wert obligatorisch.[373] Für die alltägliche Nutzung von Kryptowährungen stellt dies ein Problem dar, denn welcher Käufer möchte heute etwas mit einer Kryptowährung kaufen, wenn womöglich der Wert morgen 20 Prozent höher liegen könnte? Und welcher Verkäufer möchte heute eine Kryptowährung annehmen, die morgen womöglich 40 Prozent weniger wert ist?[374] In diesem Zusammenhang könnte auch der Widerruf eine Rolle spielen. Bei Business to Business Geschäften (B2B) droht theoretisch ein Szenario, in dem einer der Vertragspartner nach Zahlung und nachträglicher Wertsteigerung der Kryptowährung gewillt ist, den Vertrag rückgängig zu machen, um von der Wertsteigerung zu profitieren. Eine mögliche Lösung könnte darin liegen, bei Vertragsschluss zu vereinbaren, dass bei Rückabwicklung des Vertrages lediglich der Wert der Kryptowährung bei Abschluss des Vertrages zählt und dieser in Euro geschuldet wird.[375]

Aus wirtschaftlicher Sicht bedeuten diese Unsicherheiten ein Abnehmen der Akzeptanz und des Vertrauens. Diese Schwankungen sind auch bei Fiat-Währungen ein Thema, allerdings aufgrund des weitaus größeren Volumens des Devisenmarktes von knapp fünf Billionen US-Dollar in einem deutlich geringeren Maße. Ende Januar 2015,

372 Vgl. Gojdka (2018) (abgerufen am 22. Nov. 2018).

373 Vgl. Schmidt B (2018) (abgerufen am 24. Nov. 2018).

374 Vgl. Sixt (2017), S. 107.

375 Vgl. Filbinger (2018) (abgerufen am 24. Nov. 2018).

als die Griechenlandkrise ihren Höhepunkt erreichte, lagen die Schwankungen der Fiat-Währungen wie Euro oder Pfund gegenüber dem US-Dollar bei maximal 17 Prozent – diese Volatilität erreicht der Bitcoin teilweise über Nacht.[376] Dennoch gibt es auf dem volatilen Kryptomarkt ebenso Währungen, die sich relativ stabil verhalten. Im Umkehrschluss gibt es aber auch Landeswährungen, die trotz der Stabilität des Gesamtmarktes regelmäßig starken Schwankungen unterliegen.[377]

Oft verhalten sich die Kryptomärkte anders als die traditionellen Aktienmärkte. Mitte November 2018 hingegen liegen sie ganz auf Linie. Grund sind die steigenden Zinsen in den USA, die womöglich auch den Sparzins und dementsprechend das Sparguthaben beeinflussen. Somit ziehen Anleger ihr Geld aus riskanten und spekulativen Anlagen ab. Dieser Vorgang ist mitverantwortlich für den schnellen Rückgang des Bitcoins um fast 2.000 US-Dollar, aber auch die automatisierten Handelsprogramme tragen ihren Teil dazu bei. Hier findet ein automatisierter Verkauf statt, sobald der Bitcoin oder eine andere Kryptowährung einen bestimmten Preis unterschreitet. Somit wollen Anleger ihre Verluste begrenzen, treiben allerdings den Preis noch weiter nach unten.[378]

Doch auch andere Gründe tragen zu der Volatilität bei. Zum einen sind dort Unsicherheiten im Markt, verursacht durch die Schließung und den Konkurs bekannter Dienstleister, wie der Bitcoin-Handelsplattform Mt.Gox, oder durch die Verbindung der kriminellen Silk Road Plattform zu Kryptowährungen.[379] Die bekannte Handelsplattform Coinbase ging Vorwürfen nach, dass Mitarbeiter Insiderhandel betrieben haben, um die Nachfrage nach Bitcoin Cash anzuheizen.[380] Diese Meldungen verbreiten sich in der heutigen Zeit schnell und führen zu direkten Reaktionen des Marktes. Dabei reichen schon spekulative Meldungen, wie dass die Rockefeller-Familie in Kryptowährungen einsteigen möchte.[381] Zum anderen sind Kryptowährungen doch abhängiger von staatlichen Regierungen, als von vielen angenommen. Es gibt eine Verbindung zwischen Kursverläufen und staatlichen Eingriffen. Beispiele dafür sind Eingriffe der

376 Vgl. Sixt (2017), S. 107.

377 Vgl. Schmidt B (2018) (abgerufen am 24. Nov. 2018).

378 Vgl. Gojdka (2018) (abgerufen am 24. Nov. 2018).

379 Vgl. Sixt (2017), S. 107.

380 Vgl. Heun (2018), S. 148.

381 Vgl. Kilic (2018) (abgerufen am 24. Nov. 2018).

südkoreanischen Regierung, die die Anonymität des Bitcoin-Netzwerkes reduzieren sollen sowie das Vorgehen der amerikanischen Börsenaufsicht gegen ICOs.[382]

Ein weiterer Grund für die Volatilität liegt darin, dass der Markt sich erst richtig definieren und finden muss. Niemand weiß, was der richtige Wert für beispielsweise einen Bitcoin ist. Was ist überteuert? Wann lohnt sich der Einstieg? Welcher Wert stellt den richtigen oder idealen Wert einer Kryptowährung dar? Zudem besitzen Kryptowährungen keinen intrinsischen Wert und veräußern keine Produkte. Das macht eine richtige Bewertung schwierig. Daher sind Kryptowährungen nach wie vor schwankungsanfällig gegenüber der Marktstimmung und der medialen Berichterstattung.[383]

Der Bitcoin und andere Kryptowährungen durchlaufen derzeit noch einen regelmäßigen Zyklus. Dieser stellt sich so dar, dass mediale Aufmerksamkeit und erhöhte Nachfrage zu einem Preisanstieg führen, wodurch wiederum neue Investoren und Interessenten angezogen werden. Durch die weitere Preissteigerung realisieren die ersten Anleger hohe Gewinne – dieser Abverkauf führt dann anschließend wieder zu einem Preisverfall.[384] Erst mit zunehmender Adaption der Technik und steigender Marktkapitalisierung ist mehr Stabilität zu erwarten.[385] Dabei nimmt das Vertrauen der Langzeitinvestoren eine wichtige Rolle ein.[386]

6.5 Fehlende zentrale Instanz und rechtliche Unsicherheiten

Die Blockchains der Kryptowährungen gehören keiner zentralen Stelle und unterliegen somit auch keiner Kontrolle. Dies macht sie besonders für Kriminelle interessant, die nahezu ungestört ihre Geschäfte abwickeln können.[387] Neben der Kriminalität ist das weit größere Problem, dass niemand zentral Entscheidungen treffen kann und sich die Implementierung notwendiger Updates äußerst schwierig gestaltet. Der Grund dafür liegt in der dezentralen Struktur und darin, dass die Mehrheit der Teilnehmer diesem Update zustimmen muss.[388] Dass die Blockchain nicht durch eine Instanz komplett

382 Vgl. Heun (2018), S. 149.

383 Vgl. Wozke (2018) (abgerufen am 24. Nov. 2018).

384 Vgl. Kilic (2018) (abgerufen am 24. Nov. 2018).

385 Vgl. Sixt (2017), S. 107.

386 Vgl. Kilic (2018) (abgerufen am 24. Nov. 2018).

387 Vgl. Glücklich A (2017), S. 38.

388 Vgl. Hosp B (2018), S. 82.

kontrolliert werden kann, ist einerseits ein enormer Vorteil und wird zudem noch unter Kapitel 7 als positiver Aspekt erwähnt. Andererseits gibt es oft so viele unterschiedliche Meinungen wie Teilnehmer und die Dezentralität führt zu einer gewissen Starrheit des Systems.[389] Ein Beispiel dafür war der SegWit im Bitcoin-Netzwerk. Allen war bewusst, dass aufgrund des Alters und der technischen Eigenschaften der Bitcoin dringend ein Update benötigte. Nichtsdestotrotz diskutierte das Netzwerk jahrelang, bis sich im Mai 2017 die einflussreichsten Personen schließlich doch noch einigen konnten.[390] Findet ein Netzwerk keinen gemeinsamen Konsens, kommt es zu den Forks der Blockchain, wie es jetzt beispielsweise bei Bitcoin Cash der Fall ist.[391]

Die Dezentralität ist somit Fluch und Segen zugleich. Dringend notwendige Updates durchlaufen lange Diskussionsprozesse, während in der Zwischenzeit womöglich eine andere Kryptowährung die eigene Stellung einnimmt. Auch für Start-Ups und Unternehmen stellt dies ein Problem dar, solange sie keine eigene Blockchain implementiert haben. Veränderungen, die auf das Unternehmen negativen Einfluss haben, könnten durch eine Mehrheitsentscheidung der Community getroffen werden, ohne dass das Unternehmen dagegenwirken könnte.[392]

Durch die fehlende zentrale Instanz gibt es, abgesehen durch die Verschlüsselung durch Kryptografie, keinerlei Sicherheitsanker. Es gab in der Vergangenheit bereits eine Vielzahl von Hackerangriffen und Insolvenzen großer Plattformen, wie der von Mt.Gox. Das dabei gestohlene Vermögen ging nahezu komplett verloren. Geht in Europa beispielsweise eine Bank insolvent, greifen als Absicherungen sogenannte Einlagensicherungsfonds, um das Vermögen der Sparer zu schützen.[393]

Darüber hinaus bestehen nicht zuletzt durch die Dezentralität erhebliche rechtliche Risiken und Unsicherheiten. Wie bereits ausführlich in Kapitel 5 dargestellt, gibt es derzeit wenige rechtliche Grundlagen, die ein konkretes Vorgehen vorgeben. Aufsichtsbehörden beschäftigen sich erst seit einigen Jahren intensiv mit Kryptowährungen, daher sind zukünftig weitere Anpassungen der Gesetze zu erwarten. Die Schwierigkeit

389 Vgl. Hosp B (2018), S. 82.

390 Vgl. Glücklich A (2017), S. 38 f.

391 Vgl. Hosp B (2018), S. 82 f.

392 Vgl. Glücklich A (2017), S. 39 f.

393 Vgl. Kreditkarten (o. D.) (abgerufen am 25. Nov. 2018).

vorher wird sein, die unterschiedlichen juristischen Interpretationen zu einzelnen Sachverhalten mit Kryptowährungen richtig einordnen zu können.

6.6 Sicherheit

Die Blockchain selbst gilt als sicheres System, welches durch ein aufwändiges kryptografisches Verfahren vor Manipulation und Betrug geschützt ist.[394] Bei der Sicherheit des Einzelnen sieht dies anders aus. Bei Verlust des privaten Schlüssels gehen alle damit verknüpften Kryptowährungen verloren. Es gibt keine zentrale Stelle, die einem dabei hilft, den Zugriff auf die Geldbörse wiederzuerlangen. Im Unterkapitel 4.3 wurden bereits einige Wallets vorgestellt. Menschen neigen dazu, den bequemsten und in diesem Fall unsichersten Weg zu gehen und ihre privaten Schlüssel auf dem Computer oder auf einem Server zu speichern. Dies macht sie anfällig für Hacker. Zudem werden Passwörter und PINs oft vergessen.[395]

Insbesondere Hackingangriffe zählen zu den Faktoren, die das Wachstum von Kryptowährungen bremsen.[396] Dabei zielen die Angriffe weniger auf die Netzwerke und Blockchains selbst, sondern vielmehr auf Wallets und Handelsplattformen.[397] Einer der bekanntesten Hacks fand auf die angesprochene Kryptobörse Mt.Gox statt, die daraufhin Insolvenz anmeldete. Dabei verloren etwa 25.000 Kunden rund 650.000 Bitcoins – ein heutiger Wert von mehreren Milliarden US-Dollar. Immerhin wurden Ansprüche der Geschädigten im Wert von 400 Millionen US-Dollar anerkannt.[398] Zuvor wurden bei einem Hack derselben Plattform im Jahr 2011 bereits 2.000 Bitcoins gestohlen, was damals fast acht Prozent der bis dahin geminten Bitcoins entsprach. Der Markt wurde anschließend mit gestohlenen Bitcoins geflutet, was dazu führte, dass der Kurs innerhalb kürzester Zeit auf 0,01 US-Dollar einbrach.[399] Auch andere große Börsen wie Coincheck, Nicehash oder Kraken verloren durch Hackingangriffe hohe Summen an Kryptowährungen, insbesondere Bitcoins.[400]

---

394 Vgl. Glücklich A (2017), S. 36.

395 Vgl. Glücklich A (2017), S. 37.

396 Vgl. Sixt (2017), S. 92.

397 Vgl. Heun (2018), S. 156.

398 Vgl. Heun (2018), S. 157.

399 Vgl. Sixt (2017), S. 92.

400 Vgl. Heun (2018), S. 157 f.

Für Hacker sind Kryptowährungen insbesondere durch die Unumkehrbarkeit der Transaktionen und durch die Pseudoanonymität ein interessantes Ziel. Einer Studie zufolge waren bereits knapp die Hälfte der 40 ursprünglich gegründeten Kryptobörsen bis zum Jahr 2013 wieder geschlossen – teilweise verschwanden sie mit dem angelegten Vermögen. Beim Bitcoin wird davon ausgegangen, dass knapp 15 Prozent der Coins durch Betrug, Diebstahl oder Fehlbuchungen nicht mehr bei ihrem rechtmäßigen Besitzer sind.[401]

Neben Bitcoin werden auch andere Kryptowährungen, wie beispielsweise Ethereum, immer wieder Ziel von Hackerangriffen. Nahezu alle größeren Angriffe konnten hierbei durch Sicherheitslücken in Smart Contracts ausgeführt werden.[402] Dazu zählt auch der bisher größte Angriff im Juni 2016, als aus der DAO über Lücken in den darin verwendeten Smart Contracts 3,6 Millionen Ether gestohlen wurden, was damals knapp 15 Prozent aller im Umlauf befindlichen Ether-Tokens ausmachte.[403] Generell gibt es bei Smart Contracts neben rechtlichen auch noch eine Vielzahl an technischen Unsicherheiten. Das Problem dabei ist, dass viele Lücken erst nach Angriffen gefunden werden und niemand so richtig weiß, wie diese überhaupt aussehen. Nach der Analyse von fast einer Million Smart Contracts fand eine Forschergruppe heraus, dass fast 34.000 Verträge Schwächen aufwiesen – für eine neue und in weiten Teilen unerprobte Technologie eigentlich eine gute Quote. Haben diese Lücken allerdings einen Diebstahl in Höhe des DAO-Hacks zur Folge, relativiert sich diese Quote schnell wieder.[404]

Darüber hinaus besteht bei Kryptowährungen mit Mining theoretisch die Gefahr eines sogenannten 51-Prozent-Angriffs. Dabei besitzt ein Miner oder ein Miningpool 51 Prozent der Rechenleistung des Netzwerkes und kann somit die Bestätigung der Transaktionen verhindern oder die Blockchain forken.[405] Damit ist keine Dezentralität vorhanden und derjenige mit 51 Prozent kann seine eigene Blockchain durchsetzen. Zudem besteht das Problem des Double Spendings – mit der Mehrheit der Rechenleis-

401 Vgl. Sixt (2017), S. 93.

402 Vgl. New Alchemy (2018) (abgerufen am 27. Nov. 2018).

403 Vgl. Glücklich B (2017), S. 10.

404 Vgl. Orcutt (2018) (abgerufen am 27. Nov. 2018).

405 Vgl. Sixt (2017), S. 105.

tung können Transaktionen beliebig umgeleitet oder umgekehrt werden. Normalerweise prüft das dezentrale Netzwerk, ob ein Coin bereits ausgegeben wurde. Bei einem 51-Prozent-Angriff kann dieser Coin simultan an mehrere gleichzeitig ausgegeben werden und somit das komplette Ökosystem der Kryptowährung durcheinanderbringen.[406] Bei vielen bekannten Kryptowährungen ist ein solcher Angriff relativ unwahrscheinlich, wenn auch mit Blick auf die Verteilung der Mining-Pools nicht unmöglich. Dass einzelne Personen 51 Prozent der Rechenleistung im Bitcoin-Netzwerk stellen, ist ausgeschlossen. Doch bei einem Blick auf die Verteilung der Hashrate wird deutlich, dass die vier größten Mining-Pools über 50 Prozent der Rechenleistung stellen.[407] Somit ist die Gefahr durchaus real. Bei kleineren Altcoins sind solche Angriffe in der Vergangenheit bereits vorgekommen.[408]

Viele Maßnahmen, Kryptowährungen sicherer zu gestalten, hängen in erster Linie von den Nutzern ab. Cyberkriminalität zeichnet sich zudem auch dadurch aus, dass Kriminelle versuchen, menschliche Schwächen auszunutzen, beispielsweise über gefälschte Webseiten oder E-Mails.[409] Zudem wird die Entwicklung der sogenannten Zwei-Faktor-Authentifizierung vorangetrieben. Dabei wird die Identität des Nutzers durch zwei unabhängige Faktoren nachgewiesen, die nur der jeweilige Nutzer weiß. Ähnlich verhält es sich bei der Kombination aus Bankkarte und PIN.[410] Bei richtiger Aufbewahrung des privaten Schlüssels und sorgfältiger Auswahl eventueller Handelsplätze ist das Risiko, seine Coins durch Hacking komplett zu verlieren, relativ gering.

406 Vgl. BTC-Echo G (o. D.) (abgerufen am 27. Nov. 2018).

407 Vgl. Blockchain C (o. D.) (abgerufen am 27. Nov. 2018).

408 Vgl. BTC-Echo G (o. D.) (abgerufen am 27. Nov. 2018).

409 Vgl. Heun (2018), S. 153.

410 Vgl. Sixt (2017), S. 94.

7 Chancen von Kryptowährungen und Blockchain

Neben den Chancen von Kryptowährungen werden in diesem Kapitel auch wirtschaftliche Potenziale anhand von Anwendungsbeispielen dargestellt.

7.1 Kostensenkung und Effizienzsteigerung

Kryptowährungen besitzen das Potenzial, Transaktionen deutlich effizienter und kostengünstiger abzuwickeln, als es derzeit im herkömmlichen Zahlungsverkehr möglich ist. Dies liegt in erster Linie am Fehlen von Mittelsmännern und Banken, deren Gebühren und Abwicklungsprozesse wegfallen.[411] Dabei rückt der Blick von Bitcoin ab, da dort die Transaktionsgebühren zuletzt stark gestiegen sind und Transaktionen unwirtschaftlicher und langsamer werden, je kleiner sie sind. Das vorgestellte Ripple-System ermöglicht es, Transaktionen im Umfang des Visa-Netzwerks in Echtzeit zu verarbeiten. Dabei betragen die Gebühren lediglich den Bruchteils eines Cents.[412] Für die Wirtschaft bieten günstige Transaktionen in Echtzeit enorme Vorteile, insbesondere im internationalen Kontext. Aufgrund der ressourcenintensiven Abwicklung über zentrale Instanzen benötigen Überweisungen ins Ausland mehrere Tage. Auch im Inland benötigen Überweisungen zwischen unterschiedlichen Banken ein bis zwei Tage. Dadurch wird einerseits der gesamte Geschäftsprozess verlangsamt, andererseits erhöht sich das Wechselkursrisiko bei Auslandsgeschäften. Durch eine kürzere Abwicklungszeit könnten Kryptowährungen und Blockchain dieses Risiko minimieren.[413] Finden die Transaktionen in der Kryptowährung statt, muss insbesondere noch derzeit das Risiko der Volatilität der Kryptowährung beachtet werden. Vielmehr stellt in diesem Kontext die Blockchain-Technologie den herausragenden Vorteil dar.

Zudem wurde in der Masterarbeit von Alina Ley im Rahmen einer Expertenbefragung ebenfalls der Zeit- und Kostenfaktor als einer der größten Erfolgsfaktoren von Kryptowährungen identifiziert. Zeit und Kosten werden dabei als voneinander abhängig betrachtet, da langsame und ineffiziente Prozesse für Unternehmen oftmals Kosten verursachen.[414] Die vorgestellten Bezahlmethoden, wie Kreditkarten, Lastschrift oder

411 Vgl. Heun (2018), S. 138.

412 Vgl. Grinschuk (2017), S. 40.

413 Vgl. Schütte et al. (2017), S. 27 f. (abgerufen am 29. Nov. 2018).

414 Vgl. Ley (2017), S. 88.

PayPal, benötigten entweder deutlich länger, erheben unter gewissen Rahmenbedingungen hohe Gebühren oder kombinieren sogar beide Nachteile.[415] Allerdings muss hierbei noch stark zwischen den unterschiedlichen Kryptowährungen unterschieden werden.

Durch die gesteigerte Effizienz könnten Kryptowährungen sogar komplett neue Anwendungsgebiete schaffen, insbesondere im Bereich des Mirco- und Nanopayments. Bei Micropayments rückt IOTA in den Fokus, da dort über das IOTA-Token diese Art von Zahlungen wirtschaftlich, autonom und schnell abgewickelt werden können. Auch die Geschwindigkeit würde kein Problem mehr darstellen, da das IOTA-System mit mehr gleichzeitigen Nutzern sogar noch schneller wird. Auch sogenannte Nanopayments, ein bisher kaum erschließbares Anwendungsfeld, in denen lediglich Bruchstücke eines Cents transferiert werden, sind wirtschaftlich sinnvoll darstellbar.[416]

7.2 Dezentralität

Die Dezentralität wird regelmäßig als eines der wichtigsten Grundelemente von Blockchain und Kryptowährungen bezeichnet. Diese Eigenschaft bringt neben der in Kapitel 6 erwähnten Risiken zugleich zahlreiche Vorteile mit sich. Da in diesem Zusammenhang oft der Begriff Distributed-Ledger-Technologie fällt, soll dieser zuvor kurz eingeordnet werden. Distributed Ledger kann als verteiltes Kontenbuch betrachtet werden und stellt das Grundgerüst der Blockchain dar. Die Blockchain ist somit nur eine bestimmte Art von Distributed-Ledger-Technologie. Nicht jedes verteilte Kontenbuch ist eine Blockchain; erst durch die Aneinanderreihung von Blöcken entsteht diese Kette.[417]

Ein dezentrales Netzwerk ist für jeden jederzeit zugänglich. Dabei werden Daten über ein dezentrales Netzwerk von Computern verwaltet und die Abhängigkeit von Dritten entfällt. Der Aufbau findet dabei nach dem Prinzip Peer-to-Peer (P2P) statt, das heißt, die Daten gehen direkt ohne Umwege an die jeweiligen Knoten. Sensible Daten, wie beispielsweise Kontodaten bei einer Überweisung, werden an keiner zentralen Stelle gespeichert und sind so für niemanden einsehbar. Die Transaktion wandert durch das

415 Vgl. Ley (2017), S. 89.

416 Vgl. Brenneis (2017) (abgerufen am 29. Nov. 2018).

417 Vgl. Blockchainwelt C (2018) (abgerufen am 29. Nov. 2018).

Netzwerk und alle daran beteiligten Computer erledigen einen Teil der Arbeit – mit dem großen Vorteil, dass niemand auf die gesamte Transaktion zugreifen kann, da jeder Knoten nur einen äußerst geringen Teil der Daten erhält.[418]

In einem zentralen System werden Daten über einen zentralen Server verwaltet. Wenn beispielsweise eine Nachricht bei WhatsApp oder Überweisung in Euro gesendet wird, muss darauf vertraut werden, dass diese zentrale Institution die Transaktion sicher und korrekt verarbeitet und vertrauenswürdig mit den betroffenen Daten umgeht.[419] Diese Abhängigkeit war einer der zentralen Gründe für die Entstehung von Blockchain und Kryptowährungen. Hier bedeutet die Dezentralität in erster Linie, dass keine Einzelperson oder Institution Macht über das gesamte Netzwerk ausüben kann. Davon profitieren insbesondere Menschen in Ländern mit hoher Korruption, in denen zentralen Institutionen kein Vertrauen geschenkt werden kann.[420]

Auch haben deutlich mehr Menschen Zugang zu Internet und Smartphone, als zum Bankensystem. Dazu gehören auch Menschen aus Schwellenländern und ärmeren Regionen, in denen vorhandene Bankensysteme nicht immer ausreichend gut funktionieren. Für diese Bevölkerung bieten Kryptowährungen enormes Potenzial und ermöglichen eine Integration in ein neues Finanzsystem, in dem niemand aufgrund festgelegter Kriterien ausgeschlossen wird.[421]

In Venezuela ist der Bitcoin inzwischen zur wichtigsten Parallelwährung aufgestiegen. Nach jahrelanger Misswirtschaft schätzt der IWF, dass die Inflationsrate der landeseigenen Währung bis Ende 2018 bei über 2.000 Prozent liegen wird. US-Dollar sind dort nur über komplizierte Umwege zu erwerben – somit legen immer mehr Menschen ihr Vermögen in vom Staat unabhängigen Kryptowährungen an oder kaufen damit lebensnotwendige Güter.[422] Nach einem von der London School of Economics (LSE) konstru-

418 Vgl. Decentralbox (2017) (abgerufen am 29. Nov. 2018).

419 Vgl. Decentralbox (2017) (abgerufen am 29. Nov. 2018).

420 Vgl. Glücklich A (2017), S. 29.

421 Vgl. Bitcoin-Generator (o. D.) (abgerufen am 30. Nov. 2018).

422 Vgl. Fuster (2017) (abgerufen am 30. Nov. 2018).

ierten Index bietet die Dezentralität auch für weitere Schwellenländer, wie beispielsweise Argentinien, Nigeria und Indien, ein hohes zukünftiges Potenzial durch die Nutzung von Bitcoin und anderen Kryptowährungen.[423]

Trotz fehlender zentraler Instanz und daraus resultierenden Akzeptanz- und Vertrauensvorbehalten wird die Dezentralität auch in der Literatur mehrheitlich als Chance gesehen.[424] Zum gleichen Ergebnis kommt auch die Expertenbefragung durch Alina Ley.[425] Obwohl das flächendeckende Vertrauen in Kryptowährungen fehlt, ging in den letzten Jahren auch das Vertrauen in traditionelle Finanzinstitute stark zurück. Aus der Niedrigzinspolitik der EZB wurde eine Nullzinspolitik, die dafür sorgte, dass die Einlagen der Sparer nach und nach von der Inflation förmlich aufgefressen wurden. Diese Politik der EZB steht nach wie vor in der Kritik und führt dazu, dass die Dezentralität zunehmend als positiver Faktor wahrgenommen wird.[426]

Nicht zuletzt erhöht die Dezentralität die Sicherheit des Netzwerkes. Die Daten liegen nicht zentral auf einem Server, sondern sind auf der Blockchain in unzähligen Datenbanken weltweit gespeichert.[427] Bei einem Hackingangriff auf einen Zentralserver sind im schlimmsten Fall alle Daten gestohlen oder zerstört. Ähnliche Probleme bestehen lediglich bei einem Angriff auf große Kryptobörsen, nicht aber bei der Blockchain selbst.[428] Zudem erhöht sich die Robustheit des Netzwerkes. Der Ausfall weniger Knotenpunkte hat keinerlei Auswirkungen auf die Leistung des Gesamtnetzwerkes, während ein Serverausfall in einer Bank zur Folge haben kann, dass tausende Kunden keinen Zugriff auf ihr Geld haben.[429]

Neben den genannten Vorteilen ist für viele Benutzer zudem die Dezentralität auch ein übergeordnetes Anliegen. Die Zukunft der sicheren Datenübertragung im Internet liegt in vielen kleinen Einheiten, die für sich selbst entscheiden können. Große, zentrale Einheiten, die die Kontrolle haben, werden zukünftig an Relevanz verlieren. Sich durch

423 Vgl. Hileman (2016) (abgerufen am 30. Nov. 2018).

424 Vgl. bspw. Thiemann (2017), S. 14 f., Glücklich A (2017), S. 29 f.

425 Vgl. Ley (2017), S. 92 f.

426 Vgl. Schickentanz (2018) (abgerufen am 30. Nov. 2018).

427 Vgl. Glücklich A (2017), S. 29.

428 Vgl. Glücklich A (2017), S. 30.

429 Vgl. Thiemann (2017), S. 18.

Kryptowährungen bietende Chancen wie Effizienzgewinne, Fälschungssicherheit und Schutz vor Cyberattacken sind nicht von der Hand zu weisen.[430]

Nichtsdestotrotz ist es utopisch, anzunehmen, dass in naher Zukunft alle Daten verschlüsselt und schnell über dezentrale Netzwerke versendet werden. Damit zukünftig Unternehmen vermehrt auf dezentrale Technologien setzen, müssen noch viel mehr Menschen von den Vorteilen überzeugt, sowie bestehende Nachteile gemindert werden.

7.3 Transparenz und Anonymität

Transparenz und Anonymität sind weitere wichtige Vorteile von Blockchain und Kryptowährungen. Jeder Teilnehmer kann alle Transaktionen im Netzwerk einsehen. Je nach Anwendung ist dies mehr oder weniger gewünscht – je weiter Blockchain und Kryptowährungen in den wirtschaftlichen Kontext rücken, desto eher haben Unternehmen daran Interesse, nicht jede Information (wenn auch verschlüsselt) auf der Blockchain transparent für alle zu speichern.[431] Im Bitcoin-Netzwerk ist es beispielsweise möglich, alle vergangenen Transaktionen und Kontostände jederzeit einzusehen.[432] Durch diese Transparenz entsteht eine gewisse Datenintegrität und Betrug kann schnell aufgedeckt werden. Manipulationen sind nahezu unmöglich, da diese sofort im Netzwerk auffallen würden.[433] Die vorgestellten etablierten Zahlungsmethoden weisen diese Transparenz nur teilweise auf. Es ist zwar möglich, Kontobewegungen nachzuvollziehen, allerdings nur, wenn der Zugang zu diesen Informationen gegeben ist. Während Falschgeld in Form von Bargeld durchaus einige Zeit unerkannt bleiben kann, ist dies im transparenten Netzwerk einer Kryptowährung so gut wie unmöglich.[434]

Transparenz in Finanzflüssen wird nicht von jedem zu jeder Zeit gewünscht. Eine sinnvolle Anwendung liegt in der Zahlung von Fördergeldern oder generell in der Zahlung öffentlicher Gelder. Möchte die Kreditanstalt für Wiederaufbau (KfW) beispielsweise

430 Vgl. Koenig (2017), S. 46.

431 Vgl. Thiemann (2017), S. 18 f.

432 Vgl. Thiemann (2017), S. 19.

433 Vgl. Ley (2017), S. 95.

434 Vgl. Ley (2017), S. 95.

den Bau von Schulen in Mosambik unterstützen, wäre dies über Blockchain und Kryptowährungen transparent darstellbar. Beteiligte Förderer und Ministerien könnten überblicken, wohin welche Gelder fließen. Zeitgleich entsteht bei Zahlung in Form von Kryptowährungen der Vorteil, dass ein eventuell unzureichendes Banken- und Finanzsystem im Ausland keine negativen Auswirkungen hätte. Womöglich korrupte Regierungen könnten zudem nicht auf das Geld zugreifen.[435]

Trotz der Transparenz der Transaktionen sind die einzelnen Identitäten der Teilnehmer im Netzwerk nicht transparent und es werden keine persönlichen Daten gespeichert.[436] Da sich lediglich die Bewegungen der Kryptowährungen festhalten lassen, eine Zuordnung zu einer realen Person aber nicht gegeben ist, wird von sogenannter Pseudonymität gesprochen.[437] Allerdings lassen sich, wie bereits festgestellt, mit gewissem Aufwand, durch Rückrechnungen, Rückschlüsse auf die Identität eines Nutzers ziehen.[438]

Auf der einen Seite ist es positiv zu bewerten, dass im Gegensatz zu vielen anderen Services im Internet, bei Kryptowährungen die Identität nicht preisgegeben werden muss.[439] Auf der anderen Seite werden Kryptowährungen durch die Anonymität oft mit illegalen Aktivitäten in Verbindung gebracht – auch dies führt nicht zuletzt zu geringer Akzeptanz. Dass dieses Argument falsch ist, zeigt eine aktuelle Studie, laut derer lediglich ein Prozent aller Transaktionen mit Kryptowährungen zu illegalen Zwecken durchgeführt werden, während es bei Transaktionen in Fiat-Währungen vier Prozent sind.[440] Vielmehr begünstigt die Blockchain-Technologie durch ihre Transparenz die Dokumentation möglicher Straftaten.[441] Verbrechen, wie Geldwäsche und Drogenhandel mit Kryptowährungen, wurden in der Vergangenheit bereits anhand der Transaktionshistorie aufgeklärt. Dies wäre mit Fiat-Währungen deutlich komplizierter und zeigt

435 Vgl. Rauschenberger (2017) (abgerufen am 01. Dez. 2018).

436 Vgl. Thiemann (2017), S. 19.

437 Vgl. Passwort-Generator (o. D.) (abgerufen am 01. Dez. 2018).

438 Vgl. Hosp B (2018), S. 71 f.

439 Vgl. Hosp B (2018), S. 71.

440 Vgl. Hosp (2018) (abgerufen am 01. Dez. 2018).

441 Vgl. Hosp B (2018), S. 72.

einmal mehr, dass Kryptowährungen nicht zwingend für illegale Geschäfte geeignet sind.[442]

Das Unterkapitel 7.5 zeigt, wie die Transparenz im wirtschaftlichen Kontext positiv in Erscheinung tritt.

7.4 Vorreiterrolle

Eine nicht zu unterschätzende Chance für Unternehmen stellt das Einnehmen der Vorreiterrolle in einem neuen technologischen Umfeld dar. Während Länder wie die Schweiz oder Liechtenstein bereits durch eine liberalere Haltung gegenüber Kryptowährung in der Öffentlichkeit stehen, sind Unternehmen bisher kaum in Erscheinung getreten. Die große Mehrheit verzichtet bisher generell auf Projekte mit Blockchains, da keine Anwendungsfälle gesehen werden und es zudem an qualifiziertem Personal fehlt.[443]

Im ersten Schritt müssen natürlich die Risiken abgewägt sowie Sicherheitsmaßnahmen implementiert werden. Grundsätzlich können Unternehmen, die Kryptowährungen im Austausch gegen Waren oder Dienstleistungen annehmen, ihren Bekanntheitsgrad deutlich steigern.[444] Dies gilt selbst noch für den Bitcoin, der bisher, abgesehen von einigen Ländern, von wenigen Unternehmen akzeptiert wird. Wenn selbst der Bitcoin als älteste Kryptowährung noch Potenzial für eine Vorreiterrolle bietet, kann abgeleitet werden, welche Chancen technisch weiterentwickelte Kryptowährungen wie Ethereum oder Ripple bieten.[445] Durch den gesteigerten Bekanntheitsgrad lassen sich viele junge und technikbegeisterte Neukunden gewinnen, die zu einer signifikanten Steigerung des Umsatzes und Gewinns führen können. Zudem besteht die Chance, dass sich komplett neue Geschäftsfelder ermöglichen, in denen die jeweiligen Unternehmen dann einen enormen Vorsprung hätten.[446]

Dabei ist es wichtig, herkömmliche Zahlungsmethoden nicht direkt ersetzen zu wollen, sondern vielmehr Kryptowährungen als weiteres Zahlungsmittel zu akzeptieren, um für

---

442 Vgl. Hosp (2018) (abgerufen am 01. Dez. 2018).

443 Vgl. Streim, Britze (2018) (abgerufen am 02. Dez. 2018).

444 Vgl. Filbinger (2018) (abgerufen am 02. Dez. 2018).

445 Vgl. Kryptomagazin (o. D.) (abgerufen am 02. Dez. 2018).

446 Vgl. Filbinger (2018) (abgerufen am 02. Dez. 2018).

einen breiten Kundenbereich optimal aufgestellt zu sein. Das Potenzial der Vorreiterrolle hat auch der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) erkannt und möchte Deutschland und deutsche Unternehmen zum Vorreiter in Sachen Blockchain und Kryptowährungen machen. Der Verband spricht sich für Förderprogramme sowie Ausbildungs- und Studienprogramme zum Thema Blockchain und Kryptowährungen aus. Hierbei wird auch die Politik in die Verantwortung genommen.[447]

7.5 Anwendungsspezifische Chancen und Potenziale

Generell werden die unterschiedlichen Anwendungsbereiche von Kryptowährungen zu den potenziellen Erfolgsfaktoren gezählt. Dazu gehören die Nutzung als Wertanlage für Privatpersonen, die Abwicklung wirtschaftlicher Transaktionen in Kryptowährungen sowie die Nutzung der Blockchain-Technologie zur Modellierung komplexer Prozesse innerhalb einer Wertschöpfungskette.[448]

Richtig verdeutlichen lassen sich die Chancen, insbesondere der Smart Contracts, erst anhand praktischer Anwendungsbeispiele in Branchen, die laut Studien ein hohes Anwendungspotenzial für Kryptowährungen und Blockchain bieten.

Eine PwC-Studie zeigt, dass neben Gesundheitswesen, Energiewirtschaft und Industrie besonders in der Finanzbranche die größten Potenziale für Kryptowährungen und Blockchain gesehen werden. Dazu wurden 600 Fachexperten und Führungskräfte befragt.[449] Diese Branchen sind zudem am ehesten von der sogenannten Disruption betroffen, die von Kryptowährungen ausgeht. Dieses Thema gewann für viele Unternehmen erst wieder durch Kryptowährungen an Relevanz. Disruption leitet sich dabei von dem englischen Wort disrupt (zu Deutsch: zerstören, zerschlagen) ab und beschreibt einen Prozess, der insbesondere mit der Digitalisierung in Verbindung gebracht wird. Dabei wird ein bestehendes Geschäftsmodell oder ein gesamter Markt durch eine stark wachsende Innovation abgelöst. Eine disruptive Innovation führt dabei, anders

447 Vgl. Streim, Britze (2018) (abgerufen am 02. Dez. 2018).

448 Vgl. Ley (2017), S. 95 f.

449 Vgl. PwC A (2018) (abgerufen am 03. Dez. 2018).

als eine Innovation im klassischen Sinne, zu einer starken Umstrukturierung und Veränderung des bestehenden Modells oder der Technologie.[450]

Für Unternehmen bietet diese Disruption Chancen, aber auch Risiken. Wichtig ist, dass die jeweiligen Branchen rechtzeitig reagieren und Frühaufklärung betreiben, um von veränderten Rahmenbedingungen nicht aus dem Markt gedrängt zu werden.[451] Nehmen sich Unternehmen diesen Änderungen rechtzeitig an, besteht die Chance, eine Vorreiterrolle in einem stark veränderten Marktumfeld einzunehmen. Neben dem Potenzial, Teile der Geschäftsmodelle einer Organisation in Frage zu stellen, bieten Kryptowährung und Blockchain auch die Möglichkeit, komplett neue Geschäftsmodelle zu entwickeln, die ohne diese Technologie gar nicht umsetzbar wären.[452]

Ein Beispiel stellen die Finanzbranche und das Internet der Dinge dar. Hierbei entsteht eine völlig neue Art des Zahlungsverkehrs – autonome Maschinen bezahlen andere Maschinen. Verpassen Finanzunternehmen den Anschluss, kann dies sowohl negative Auswirkungen auf die Zukunft als auch auf die gegenwärtigen Geschäftsfelder haben. Hat sich dieses neue Geschäftsfeld erst einmal etabliert, könnte auch der bestehende Zahlungsverkehr der Banken in Frage gestellt werden.[453]

Bevor anhand einzelner Anwendungsfelder die Chancen von Kryptowährungen dargestellt werden, sollen zuvor die Smart Contracts näher definiert werden. Smart Contracts sind intelligente, digitalisierte Verträge und stellen einen zentralen Bestandteil der Plattform Ethereum dar.[454] Durch die damit verbundene Automatisierung lassen sich viele Prozesse optimieren und teilweise auch um eine Prüfinstanz erleichtern, wenn die Konsistenz der Informationen gegeben ist. Dabei spezifizieren Smart Contracts, was bei einer Transaktion zu prüfen ist und welche Folgeaktivitäten ausgelöst werden.[455] Dies ist prinzipiell als einfache Wenn-Dann-Beziehung vorstellbar. In der Praxis wird dabei in der Regel ein festgelegter Betrag an ETH an den Transaktionspartner überwiesen. Bieten andere Blockchains die technischen Voraussetzungen

450 Vgl. Gründerszene (o. D.) (abgerufen am 03. Dez. 2018).

451 Vgl. Ley (2017), S. 103.

452 Vgl. Schütte et al. (2017), S. 21 (abgerufen am 03. Dez. 2018).

453 Vgl. Beckmann & Partner CONSULT (2018) (abgerufen am 03. Dez. 2018).

454 Vgl. Glücklich B (2017), S. 18.

455 Vgl. Schütte et al. (2017), S. 19 (abgerufen am 04. Dez. 2018).

für Smart Contracts, kann die Abwicklung theoretisch auch in einer anderen Kryptowährung erfolgen.[456]

Zudem ergibt sich die Chance der Entwicklung der bereits kurz vorgestellten dezentralisierten Applikationen (dApps). Herkömmliche Apps, wie sie bereits millionenfach in den bekannten App-Stores von Android und Apple zu finden sind, werden von einzelnen Anbietern vertrieben und weiterentwickelt. Die Daten laufen gesammelt zu den großen Anbietern wie Facebook oder Google und gleichzeitig noch über den jeweiligen App-Store. Die dApps hingegen werden dezentral auf jedem Knotenpunkt in der Blockchain simultan ausgeführt. Die Geschwindigkeit ist aktuell noch geringer als bei herkömmlichen zentralen Servern, bietet aber gleichermaßen Vorteile wie beispielsweise Manipulationssicherheit und hohe Fehlertoleranz.[457] Ethereum kann im Gegensatz zu Bitcoin vielmehr als dezentralisierte Plattform verstanden werden, die anbietet, blockchainbasiert Smart Contracts auszuführen und dApps zu entwickeln. Die Kryptowährung ETH ist dabei ebenfalls ein Mittel zum Zweck, um Transaktionen abzuwickeln.[458]

7.5.1 Beispiel Supply Chain Management

Das Supply Chain Management stellt ein spannendes Anwendungsfeld dar, da die wertschöpfenden Prozesse zunehmend unternehmensübergreifend stattfinden. Eine Vielzahl an Partnern bestehend aus Lieferanten, Herstellern, Händlern, Logistik- sowie Finanzdienstleistern, zwischen denen Leistungsvereinbarungen existieren, benötigen sichere Lösungen für den Austausch verschiedener Daten und für die Transaktionen von Zahlungen.[459] Daneben gehören Transparenz und Rückverfolgbarkeit zu wichtigen Grundlagen in der Logistik.[460] In der gegenwärtigen Praxis zählen in der Supply Chain intransparente Daten, manuelle Arbeitsschritte mit viel Papierarbeit, Schnittstellenprobleme und fehlende Transporthistorien allerdings zum Alltag.[461] Die dezentralen Blockchains mit ihren unveränderlichen Transaktionsdaten versprechen Abhilfe.

---

456 Vgl. Glücklich B (2017), S. 18.

457 Vgl. Bender (2018) (abgerufen am 04. Dez. 2018).

458 Vgl. BTC-Echo D (o. D.) (abgerufen am 04. Dez. 2018).

459 Vgl. Schütte et al. (2017), S. 25 (abgerufen am 04. Dez. 2018).

460 Vgl. IBM (o. D.) (abgerufen am 04. Dez. 2018).

461 Vgl. Herzog, Oest (2017) (abgerufen am 04. Dez. 2018).

Für viele Endverbraucher spielt Vertrauen eine zunehmend wichtige Rolle, aber auch Beteiligte innerhalb der Supply Chain möchten verlässliche Informationen über Qualität und Lieferstatus. Als folgendes Anwendungsszenario folgt eine Übersicht über eine mögliche Blockchain-Implementierung in einer digitalisierten Supply Chain für Wein:

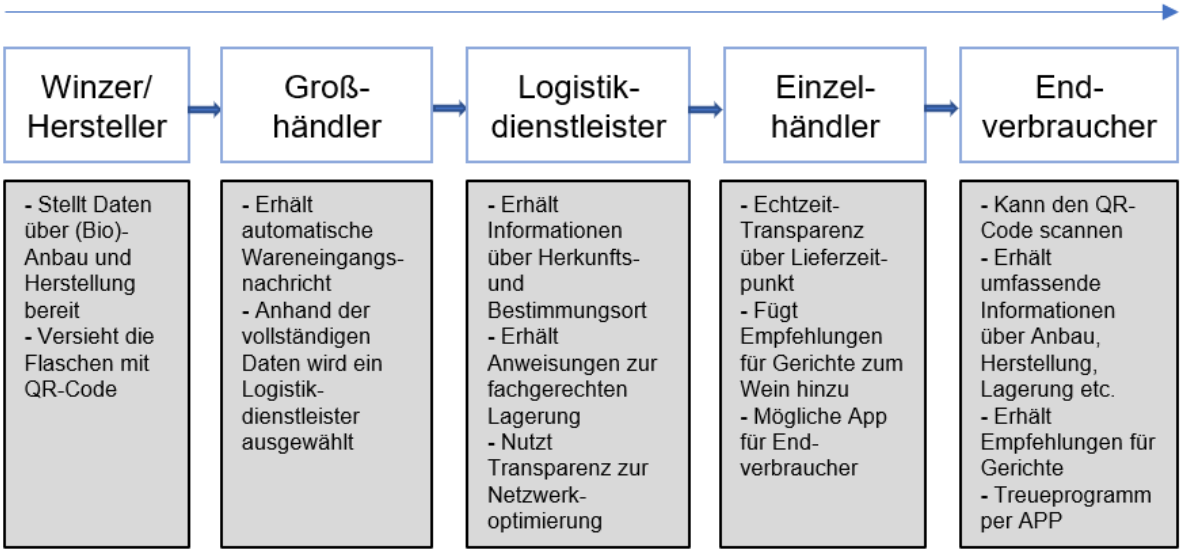

Abb. 10: Beispiel für eine blockchainbasierte Supply Chain

(Quelle: Eigene Darstellung nach Herzog, Oest (2017) (abgerufen am 04. Dez. 2018)).

Einzelne Folgeaktivitäten könnten dabei über Smart Contracts initiiert und sicher abgewickelt werden – gleichzeitig würde die Überweisung eines festgelegten Betrags von einer Kryptowährung (beispielsweise ETH) an den Transaktionspartner ausgelöst werden.

Dieses Prinzip lässt sich auf viele Produkte übertragen, bei denen die Qualität und Herkunft noch relevanter sind. Durch die Revisionssicherheit der Blockchain entsteht eine höhere Glaubwürdigkeit als beispielsweise bei dem herkömmlichen Track & Trace. Zusätzlich können Informationen auf der Blockchain ergänzt werden und sie bietet ein hohes Automatisierungspotenzial. Dadurch ist es beispielsweise möglich, bei Wareneingängen die Rechnungen automatisiert abzuwickeln. In der Hafenlogistik gibt es Anwendungsmöglichkeiten in Form von digitalisierten Frachtpapieren oder automatisierten Zollabwicklungen.[462] Die Möglichkeiten kennen nahezu keine Grenzen. Selbst

[462] Vgl. Herzog, Oest (2017) (abgerufen am 04. Dez. 2018).

Qualitätsnachweise bei wertvollen Metallen, bei denen hochauflösende Bilder von der Metallbeschaffenheit vom Hersteller in die Blockchain geladen werden, sind denkbar. Somit kann der Käufer die Bilder mit dem Produkt vergleichen, um festzustellen, ob es sich um eine Fälschung oder minderwertiges Material handelt, welches womöglich während des Transportes ausgetauscht wurde. Durch die Datenintegrität der Blockchain kann das Foto nachträglich nicht mehr verändert werden.

Im Bereich der Containerlogistik arbeitet IBM zusammen mit der Reederei Maersk an einer blockchainbasierten Lösung zur Verfolgung ganzer Schiffscontainer und deren Inhalte.[463] Diese auf der IBM-Blockchain basierende Plattform mit dem Namen Tradelens hat als Ziel, viele manuelle, kostspielige und ineffiziente Prozesse anzugehen, die sich auf den gesamten weltweiten Güterverkehr auswirken. Dabei ist Tradelens allerdings nicht wie die klassische Blockchain des Bitcoins zu verstehen. Vielmehr dient sie als zentrale Informationsplattform für Versanddaten, Dokumente, Reedereien, Häfen, Spediteure und Zollbehörden – ähnlich wie Ethereum.[464] Der Nutzen geht dabei über Echtzeitdaten vom Transportstatus bis hin zu Sensordaten bei Kühlcontainern, die jederzeit für jede involvierte Partei abrufbar sind. In Kombination mit Smart Contracts bestehen Möglichkeiten wie beispielsweise das automatische Aussteuern einer Strafzahlung bei Unterbrechung der Kühlkette oder einem Warnhinweis bei Unterschreitung einer bestimmten Temperatur.

Bei derzeit ungefähr 100 beteiligten Organisationen und knapp 155 Millionen erfassten Versandvorgängen kann für Tradelens ein positives Fazit gezogen werden. Durch Anwendung von Smart Contracts konnten beispielsweise Dokumentenfehler und Informationsbarrieren nahezu ausgeschaltet werden. Ein Handelsdokumentmodul stellt durch einen unwiderlegbaren Prüfpfad die effiziente Zusammenarbeit mit Zollbehörden und Regierungen sicher. Ein gewaltiger Vorteil – Schätzungen gehen davon aus, dass ungefähr ein Fünftel der gesamten physischen Transportkosten auf die Dokumentenabwicklung zurückgehen. Beispielsweise werden für eine Sendung von Blumen per Seefracht knapp 200 Dokumente benötigt, ausgestellt von zwei Dutzend unterschiedlichen Parteien. Bei einem handelt es sich um das sogenannte Bill-of-Lading,

[463] Vgl. Grinschuk (2017), S. 118.

[464] Vgl. Ostler A (2018) (abgerufen am 29. Sept. 2018).

also ein Frachtbrief, der normalerweise physisch weitergegeben wird. Eine einzige kleine Abweichung auf diesem Dokument kann dazu führen, dass eine komplette Warensendung aufgehalten wird und im schlimmsten Fall verdirbt. Laut Expertenschätzungen entstehen durch solche Fälle jährlich Kosten in Höhe von knapp 40 Milliarden US-Dollar.[465] Dem World Economic Forum nach könnte der Welthandel um 15 Prozent wachsen, würden alle Barrieren in internationalen Lieferketten beseitigt werden.[466]

Bei dieser Vielzahl an Vorteilen stellt sich die Frage, wieso inzwischen nicht jeder Spediteur und jede Reederei Teil eines globalen blockchainbasierten Supply Chain Netzwerkes sind. Doch so einfach ist eine Umsetzung derzeit noch nicht. Eine Hürde ist die notwendige Digitalisierung aller Bereiche innerhalb der Supply Chain. Beim Außenhandel mit außereuropäischen Ländern sind digitale Frachtpapiere noch lange kein Standard. Wenn der Hersteller seine Nachweise schon nicht digital hinterlegen kann, würde dies zu einer unvollständigen Transparenz führen. Zudem müssen alle beteiligten Unternehmen sich mit der Technologie vertraut machen und diese in ihre bestehenden digitalen Strukturen einbinden. Dies erfordert Knowhow und finanzielle Ressourcen. Zudem ist dazu eine leistungsfähige IT-Infrastruktur Voraussetzung.

Ein möglicher Ansatz für eine realistische Umsetzung in der Wirtschaft wäre eine Plattform wie Tradelens – eine zentrale Stelle, die auf der einen Seite von der ursprünglichen dezentralen Idee abrückt, auf der anderen Seite allerdings dieselben Vorteile wie Sicherheit und Transparenz bietet. Eine vorab definierte Kryptowährung könnte dabei zur Abwicklung verwendet werden. Es entsteht zwar dadurch erneut eine gewisse Abhängigkeit, allerdings wäre es utopisch anzunehmen, dass in naher Zukunft der Welthandel mit allen Beteiligten ohne zentrale Koordination stattfinden kann. Zumal es meines Erachtens auch gar nicht notwendig ist, alles komplett zu dezentralisieren – eine zentrale Steuerung durch eine vertrauenswürdige Institution würde in der Wirtschaft ebenfalls viele Vorteile schaffen. Diese Vorteile entstehen allerdings durch die Technologie und nicht durch die zentrale Institution selbst. Zumal eine komplett öffentliche Blockchain wie die des Bitcoins für die Wirtschaft auch keine zukunftsorientierte Lö-

[465] Vgl. Kolbe (2018), S. 2 (abgerufen am 30. Sept. 2018).

[466] Vgl. Ostler B (2018) (abgerufen am 29. Sept. 2018).

sung darstellt – vielmehr stellen die konsortialen Blockchains eine interessante Alternative dar. Eine mögliche Anwendung liegt beispielsweise darin, dass alle in Abbildung 10 involvierten Unternehmen durch eine solche Blockchain verbunden werden. Durch die Möglichkeit der administrativen Steuerung könnten nachträglich auch die Kunden zu diesem Netzwerk hinzugefügt werden.[467] Durch die Administration geht zwar der Open-Source-Gedanke verloren, aus Unternehmenssicht ist es allerdings verständlich, dass trotz Verschlüsselung nicht jeder auf alle Daten zugreifen kann. Zudem weist das Netzwerk durch die Begrenzung der Teilnehmer eine deutlich höhere Effizienz auf. Diese Blockchains können ganze Branchen miteinander verknüpfen und Transaktionen weltweit in Sekundenschnelle abwickeln.

7.5.2 Beispiel Finanzbranche

Auch der finanzielle Aspekt des Supply Chain Managements bietet Ansätze für den Einsatz von Kryptowährungen. Finanzprozesse in Supply Chains sind oft langsam, nicht effizient und von der eigentlichen Leistungserstellung entkoppelt. Gründe dafür sind häufig manuelle und fehleranfällige Prozesse – über die Hälfte aller Transaktionen im Bereich B2B werden basierend auf Papierrechnungen abgewickelt.[468] Durch Blockchain können diese Transaktionen unabhängig von Rechnungen über Smart Contracts abgewickelt werden. Die Blockchain speichert alle relevanten Daten unwiderruflich und verteilt diese. Die Smart Contracts überprüfen bei Ausführung diese Daten, beispielsweise Vertragsinhalte, und legitimieren selbstständig und automatisch Finanztransaktionen. Dazu kann auch gehören, dass bei Verstoß gegen hinterlegte Vertragsinhalte die Zahlung einbehalten oder eine Vertragsstrafe veranlasst wird.[469]

Ohne den Kontext des Supply Chain Managements bietet die Finanzbranche den aktuell größten Bereich mit Kryptowährungs-Projekten und Blockchain-Aktivitäten. Dies hängt auf der einen Seite damit zusammen, dass in herkömmlichen Finanztransaktionen immer Intermediäre wie beispielsweise Banken involviert sind und somit eine Abhängigkeit besteht, die immer mehr Menschen hinterfragen. Auf der anderen Seite besteht bei Finanzgeschäften eine so hohe Anforderung an Sicherheit und Vertrauen,

[467] Vgl. Schneider (2018) (abgerufen am 04. Dez. 2018).

[468] Vgl. Schütte et al. (2017), S. 25 (abgerufen am 05. Dez. 2018).

[469] Vgl. Schütte et al. (2017), S. 26 (abgerufen am 05. Dez. 2018).

wie in kaum einem anderen Bereich der Wirtschaft. Auch die Geschwindigkeit spielt im internationalen Handel eine immer wichtigere Rolle. Dauern aufgrund der Koordination zwischen verschiedenen Systemen viele Überweisungen heutzutage Stunden oder Tage, ermöglichen moderne Blockchains, beispielsweise die von Ripple, Transaktionen in Echtzeit. Das würde im internationalen Handel beispielsweise das Wechselkursrisiko minimieren. Zudem würden die hohen Gebühren für internationale Überweisungen wegfallen.[470]

Transaktionsprozesse im Kapitalmarkthandel involvieren eine große Anzahl an Akteuren, sodass kontinuierlich Daten abgeglichen und geprüft werden müssen. Dadurch entstehen Kosten und lange Transaktionszeiten. Im Wertpapierhandel können durch Blockchains diese Abwicklungszeiten nahezu vollständig vermieden werden und somit ein direkter Handel stattfinden. Der Verkäufer kann sofort bestätigen, dass er das Wertpapier besitzt und der Käufer kann die notwendige Kaufkraft nachweisen.[471] Die National Association of Securities Dealers Automated Quotations (NASDAQ), die sich zur Zeit hauptsächlich mit der Kryptowährung Bitcoin beschäftigt, hat Ende 2015 für sich entdeckt, dass sich durch die Blockchain weitaus mehr Anwendungsfälle ergeben, als durch das bloße Führen von Kryptowährungen.[472] Anfang 2016 entstand beispielsweise ein Konzept mit der estländischen Wertpapierbörse OMX Tallin Stock Exchange zum Managen der Aktionärsstimmrechte. Dabei werden mithilfe von Tokens die Stimmrechte wahrgenommen. Vorteile sind dabei Mobilität und Transparenz.[473]

Auch im Finanzbereich bieten die Smart Contracts ein großes Potenzial hinsichtlich einer wirtschaftlich sinnvollen Anwendung im Alltag. Neben den erwähnten Beispielen zur Abwicklung von Finanztransaktionen im Handel, sind auch Szenarien bei beispielsweise Leasing-Verträgen denkbar. In Zeiten von digital vernetzten Fahrzeugen ist es möglich, über Smart Contracts Leasing-Verträge so zu gestalten, dass bei mehrfachem Versäumen der Zahlung der monatlichen Rate das Fahrzeug nicht mehr anspringt. Weitere Beispiele sind das Melden von deutlich überhöhen Geschwindigkeiten an die Versicherung oder bei Unternehmensanleihen eine automatisierte Auszahlung

470 Vgl. Schütte et al. (2017), S. 27 f. (abgerufen am 05. Dez. 2018).

471 Vgl. Capital Group (2018) (abgerufen am 05. Dez. 2018).

472 Vgl. Erle (2017) (abgerufen am 05. Dez. 2018).

473 Vgl. Wagenknecht (2017) (abgerufen am 05. Dez. 2018).

von Coupons an die Anleger.[474] Die Möglichkeiten sind nahezu unbegrenzt und finden durch das angewandte Wenn-Dann-Prinzip in vielen Bereichen Anwendung.

Bei der Bezahlung im Online-Handel sind nach wie vor PayPal und Kreditkarten dominant. Das Start-Up UTrust hat es sich zur Aufgabe gemacht, die Vorzüge von PayPal mit der Sicherheit der Blockchain-Technologie zu verbinden. In erster Linie muss dazu mit interessierten Unternehmen eine Infrastruktur gestaltet werden, die die Bezahlung genauso komfortabel abwickelt, wie PayPal es bereits macht. Weitere wichtige Voraussetzungen sind, wie bereits in dieser Arbeit identifiziert, rechtliche Sicherheit, ein funktionierender Mechanismus zum Käuferschutz sowie Absicherung der Volatilität für Händler.[475]

7.5.3 Beispiel Energiewirtschaft

Auch die Energiewirtschaft befindet sich nicht zuletzt durch das Internet der Dinge und Digitalisierung in einem Umbruch. Im Vergleich zur Finanzbranche steht hier der Einfluss von Kryptowährungen und Blockchain noch ganz am Anfang. Erneut wird oft vom großen Potenzial gesprochen, beispielsweise bei der Automatisierung energiewirtschaftlicher Prozesse. Dazu gehören beispielsweise ein automatisiertes Abführen von Abgaben und Umlagen – alles transparent und sicher auf der Blockchain gespeichert.[476] Prozessbeschleunigungen führen dabei auch oft zur Reduzierung von Kosten.

Im Jahr 2017 wurde durch die Bundesregierung im Rahmen des Gesetzes zur Digitalisierung der Energiewende beschlossen, sogenannte Smart Meter für Verbraucher und Erzeuger einzuführen.[477] Diese ermöglichen jederzeit ein exaktes Auslesen der Verbrauchsdaten, stehen aber nach wie vor hinsichtlich des Datenschutzes in der Kritik. Hier würde ein Einsatz der Blockchain eine sichere und transparente Übertragung der Informationen gewährleisten – ohne Rückschlüsse auf den Verbraucher zu ziehen, da dieser weitestgehend anonym bleibt. Dadurch wäre es obsolet, den Zählerstand jährlich manuell abzulesen und es bestehen Möglichkeiten zur deutlich präziseren Vor-

474 Vgl. Winheller F (2018) (abgerufen am 05. Dez. 2018).

475 Vgl. IT Finanzmagazin (o. D.) (abgerufen am 06. Dez. 2018).

476 Vgl. Peter et al. (2017), S. 21 (abgerufen am 06. Dez. 2018).

477 Vgl. Neumann, Demidova, Kohlhoff (2017), S. 24 (abgerufen am 06. Dez. 2018).

hersage des Stromverbrauches. Somit könnten Abrechnungen flexibel angepasst werden und für die Stromanbieter führt dies letztendlich zu erhöhter Planungseffizienz, die womöglich zusätzliche Strom- oder Gasimporte überflüssig macht.[478] Derzeit wird die Stromverteilung in Verteilungszentren oft mit mindestens einem Tag Vorlauf organisiert – mit der Blockchain-Technologie wäre dies in Echtzeit möglich.

Durch die Eigenschaft moderner Blockchains, kleinste Transaktionen wirtschaftlich gestalten zu können, ergibt sich eine weitere Anwendungsmöglichkeit. Das herkömmliche Abrechnungssystem ist derzeit so gestaltet, dass sich Abrechnungen im Cent-Bereich wirtschaftlich oft nicht lohnen. Transaktionen in Kryptowährungen in Echtzeit kennen diese wirtschaftlichen Grenzen nicht. Besitzt eine Person beispielsweise eine eigene Photovoltaikanlage und produziert einige Kilowattstunden mehr als er benötigt, kann er diese an einen Nachbarn senden, der einen eigenen Stromspeicher besitzt. In den Wintermonaten, wenn die eigene Erzeugung nicht mehr ausreicht, kann er sich die gespeicherte Energie wieder einspeisen. In der Blockchain kann diese Transaktion in Echtzeit, verschlüsselt und nur transparent für die Beteiligten aufgezeichnet und verrechnet werden.[479] Über zentrale Handelsplattformen wären diese Mini-Transaktionen wirtschaftlich nicht sinnvoll – auch in der Energiewirtschaft geht die Entwicklung Richtung mehr Dezentralität und höhere Demokratisierung. Schalten sich weitere Verbraucher in den Stromtausch ein, könnten ohne großen administrativen Aufwand und Kosten kleine lokale Stromplattformen entstehen. Dadurch wird neben Geld auch Zeit eingespart. Ein solches, Microgrid (zu Deutsch: Mikronetz) genanntes Netzwerk, ist in einem Viertel in New York bereits Realität.[480]

Ein weiteres realisiertes Anwendungsbeispiel stellen die Wuppertaler Wasserwerke mit ihrem Projekt Tal.Markt dar. Auf dieser Plattform können Kunden sich ihren Mix aus Ökostrom von verschiedenen Erzeugern selbst zusammenstellen. Da aktuell aus vielen Steckdosen in deutschen Haushalten ein Mix aus Atom-, Kohle- und erneuerbaren Energien kommt, könnte eine solche Plattform Grünstromzertifikate ersetzen und Klarheit geben, woher genau der Strom kommt. Zudem wird durch die Blockchain-

[478] Vgl. Neumann, Demidova, Kohlhoff (2017), S. 25 (abgerufen am 06. Dez. 2018).

[479] Vgl. Witsch (2018) (abgerufen am 06. Dez. 2018).

[480] Vgl. Witsch (2018) (abgerufen am 06. Dez. 2018).

Technologie sichergestellt, dass keine Kilowattstunde Ökostrom doppelt verteilt werden kann.[481]

Branchenübergreifend zwischen Finanzwirtschaft, Energiewirtschaft und Mobilität gibt es bereits Ansätze im Bereich der E-Mobilität. Die E-Mobilität in Deutschland steht im Vergleich zu beispielsweise den skandinavischen Ländern noch relativ weit am Anfang. Neben zu geringer Reichweite und hohen Anschaffungskosten fallen auch die Lade- und Bezahlvorgänge unter die häufig genannten Kritikpunkte. Der Stromanbieter RWE und das Start-Up Slock.it arbeiten dazu an zwei Projekten. Die Bezahlung an der Ladestation soll per Blockchain vereinheitlicht, vereinfacht und sicher gestaltet werden. Zudem soll diese automatisiert und per App jederzeit transparent darstellbar werden. Durch eine elektronische Geldbörse (E-Wallet) im Auto werden neben der Bezahlung in Kryptowährung auch Funktionen wie automatische Zahlung der Maut und Car-Sharing geboten. Das zweite Projekt befasst sich mit der Entwicklung eines intelligenten Steckers, der nicht nur das Laden an Ladestationen ermöglichen soll, sondern an allen Orten mit einer Strominfrastruktur.[482] Auch dies entspricht dem Gedanken der Dezentralität.

Diese Entwicklungen haben auch die Branchenverbände erkannt. So empfiehlt der Bundesverband für Energie- und Wasserwirtschaft seinen Mitgliedern, sich mit der Blockchain-Technologie und den darauf basierenden Kryptowährungen zu beschäftigen.[483]

7.5.4 Beispiel öffentlicher Sektor

Für den öffentlichen Sektor stellen Kryptowährungen sowohl Chance als auch Risiko dar, da die Akteure oft als Intermediäre fungieren, die ersetzt werden könnten. Dazu gehören beispielsweise Notare bei Eigentumsübertragungen und die öffentliche Verwaltung für Register. Die bisher staatlich verwaltete Digitalisierung der Prozesse im

481 Vgl. Witsch (2018) (abgerufen am 06. Dez. 2018).

482 Vgl. Göß (2016) (abgerufen am 06. Dez. 2018).

483 Vgl. Rixecker (2017) (abgerufen am 06. Dez. 2018).

öffentlichen Sektor könnte mit der Blockchain durch eine neue private Dimension ergänzt werden. Die Anwendungsfelder sind zahlreich – folgende Gebiete werden aktuell in der Wissenschaft diskutiert:[484]

- Transparenz und Offenheit: Die öffentliche Hand und Politik sehen sich zunehmend der Herausforderung ausgesetzt, ihre Aktivitäten transparent zu gestalten. Mit diversen Open-Data-Projekten stellen Kommunen, Länder und Bund eigene Daten öffentlich zur Verfügung. Mithilfe der Blockchain wären diese Daten in ihrer Echtheit abgesichert und könnten das Vertrauen stärken – in Zeiten von vielerorts fehlendem Vertrauen gegenüber der Politik ein wichtiger Faktor. Zudem können öffentliche Haushalte ihre Einnahmen und Ausgaben transparent gestalten, sodass ein Einblick in deren Struktur gewährt wird. Den Willen zur Transparenz vorausgesetzt, wäre dies auch beispielsweise auf Spendenzahlungen oder Hilfsleistungen übertragbar, indem innerhalb der Blockchain der Verwendungszweck der jeweiligen Zahlung hinterlegt wird.
- Register und Eigentumsverhältnisse: Die Blockchain ähnelt mit ihrer nachweisbaren und transparenten Dokumentation von Transaktionen einem Register. Beispielsweise Kataster oder Grundbücher können zusätzlich von der Fälschungssicherheit profitieren. Je weniger klassischen staatlichen Strukturen selbst vertraut wird, desto geeigneter erscheint ein Einsatz der Blockchain-Technologie. Auch das Zusammenspiel verschiedener Behörden aus verschiedenen Bundesländern lässt sich erheblich vereinfachen, da Dokumente jederzeit fälschungssicher abgerufen werden können.
- Verifikation und Bestätigung: Die Integrität von Daten und Dokumenten wird heutzutage oft mit digitalen Signaturen sichergestellt. Klassische digitale Signaturen erfordern allerdings eine vertrauenswürdige Stelle, die diese ausgibt. Zusätzliche Software nimmt die Signierung vor und für maximalen Schutz werden weitere Hardware-Komponenten wie Kartenlesegeräte benötigt. Durch die Blockchain wird für jedes Dokument ein Hashwert erzeugt, der auf der Blockchain liegt. Wird nun versucht, das Dokument nachträglich zu fälschen, verän-

[484] Vgl. hierzu und im Folgenden Schütte et al. (2017), S. 31 f. (abgerufen am 06. Dez. 2018), Welzel et al. (2017), S. 18 – 22 (abgerufen am 06. Dez. 2018).

dert sich der Hashwert und der Betrug wird offensichtlich. Dadurch kann nachgewiesen werden, dass ein Dokument bei einer bestimmten Person zu einer bestimmten Zeit in einer bestimmten Fassung vorgelegen hat. Die Weitergabe des Dokumentes kann nach wie vor über klassische Kanäle erfolgen.

- Wahlen: Großes Potenzial liegt auch in Durchführung von Wahlen, wenn auch gleich diese Anwendung noch sehr weit in der Zukunft liegen vermag, da viele Länder noch immer kontroverse Debatten über Datenschutz und Manipulationssicherheit bei elektronischen Wahlen führen. Beim E-Voting (elektronische Wahlen) oder beim I-Voting (Internetwahlen) mit der Blockchain-Technologie erhält jeder Kandidat ein Wallet, das als Wahlurne dient. Jeder Stimmberechtigte wiederum erhält ein Token oder Coin, den er dann zur Wahl in das jeweilige Wallet des passenden Kandidaten transferiert. Dadurch würde die Auszählung transparent und schnell stattfinden. Jeder Stimmberechtigte kann zudem selbst prüfen, ob seine Stimme gezählt wurde. Nachteilig ist, dass ohne weiteres kryptografisches Verfahren zumindest die Ausgabestelle der Tokens oder Coins nachvollziehen kann, wer wie abgestimmt hat – ein großes Problem hinsichtlich des Wahlgeheimnisses. Insbesondere in Deutschland besitzen parlamentarische Wahlen die höchsten Ansprüche in Sachen Sicherheit und Datenschutz, sodass elektronische Wahlvorgänge über Blockchains noch weit in der Zukunft liegen.
- Bundesamt für Migration und Flüchtlinge (BAMF): Als abschließendes praktisches Beispiel dient hinsichtlich der immer noch aktuellen politischen Kontroversen das Bundesamt für Migration und Flüchtlinge. Beim sogenannten digitalen Zwilling wird von einer Person oder einem Objekt eine digitale Kopie angelegt. Mithilfe des Fraunhofer Instituts hat das BAMF ein Pilotprojekt gestartet, die Blockchain-Technologie in die Asylprozesse zu integrieren. Dazu kann neben dem Datenschutz, der insbesondere bei personenbezogenen Daten eine tragende Rolle spielt, auch die Schnelligkeit der Prozesse deutlich erhöht werden. Zurzeit sind bis zu 30 Behörden in ein Verfahren involviert.[485] Ein komplettes Asylverfahren dauert bis zu sieben Monate.[486] Dies liegt zum Großteil an der

[485] Vgl. Fridgen (2018).

[486] Vgl. Bundesregierung (o. D.) (abgerufen am 06. Dez. 2018).

> Zahl an verschiedenen Behörden, für die wiederum unterschiedliche Dokumente benötigt werden. Zudem sind diese Behörden oft nicht untereinander vernetzt. Mithilfe der Blockchain werden die Informationen des jeweiligen Antragstellers als digitale Kopie auf der Blockchain gespeichert, sodass jede Behörde jederzeit den aktuellen Stand des Verfahrens prüfen kann und erkennt, welcher Schritt zu erfolgen hat. Erweitert auf den europäischen Kontext weist die Blockchain noch deutlichere Vorteile auf, beispielsweise durch eine Plattform zur anfänglichen Registrierung. Dadurch wird transparent gespeichert, wo und wann sich eine Person erstmalig registriert hat.[487]

Es bleibt allerdings festzuhalten, dass Blockchain in staatlichen Strukturen noch weiter am Anfang steht, als in vielen wirtschaftlichen Geschäftsfeldern. Abgesehen von der in Deutschland bislang schwach ausgebauten digitalen Infrastruktur, die für eine solche behördenübergreifende Technologie notwendig wäre, gibt es auch hier noch viele rechtliche Hürden.

[487] Vgl. Fridgen (2018).

8 Mögliche Entwicklungsszenarien

In der Wissenschaft werden derzeit diverse Szenarien diskutiert, wie sich Kryptowährungen in der Zukunft entwickeln werden. Diese Entwicklung hängt maßgeblich von gewissen Einflussfaktoren und -bereichen ab, die die folgende Tabelle unter Berücksichtigung des aktuellen Standes, der Relevanz des Faktors und der Entwicklungstendenz des Faktors darstellt.

Einflussbereich	**Einflussfaktor**	**Aktuell**	**Relevanz**	**Entwicklungstendenz 2030**
Einzelhändler	Transaktionskosten	Gering	Gering	↑
	Transaktionsrisiken	Mittel	Mittel	Je nach Entwicklung ↑ oder ↓
	Akzeptanz	Gering	Hoch	↑
Konsumenten	Transaktionskosten	Gering	Hoch	↑
	Transaktionsrisiken	Mittel	Mittel	Je nach Entwicklung ↑ oder ↓
	Akzeptanz	Gering	Hoch	↑
Banken	Preisvolatilität	Hoch	Gering	↓
Zentralbanken	Systemvertrauen	Hoch	Mittel	Konstant oder ↓
Handelsplattformen	Regulierung	Gering	Hoch	↑

Tab. 2: Erwartete Entwicklungstendenzen der Einflussfaktoren

(Quelle: Eigene Darstellung nach Hungerland et al. (2017), S. 61 (abgerufen am 07. Dez. 2018)).

Die Akzeptanz nimmt weiterhin eine zentrale Rolle ein. Einige Einflussfaktoren beeinflussen sich auch untereinander. Die Akzeptanz wird beispielsweise auch von der Entwicklung der Transaktionskosten abhängen. Daraus leitet die Studie zwei mögliche Szenarien ab. Im ersten Szenario gewinnen Kryptowährungen an Relevanz und gestalten insbesondere den internationalen Zahlungsverkehr effizienter, bleiben aber aufgrund technischer Limitierungen eine Randerscheinung. Das Vertrauen in das bisherige Geldsystem bleibt bestehen, Bargeld genießt weiterhin eine hohe Beliebtheit.

Dem oft zugesprochenen Potenzial zur Revolution werden Kryptowährungen nicht gerecht.[488]

Im zweiten, weitaus unrealistischeren Extrem-Szenario nimmt die Akzeptanz stark zu und Kryptowährungen etablieren sich als allgemeines Zahlungsmittel. Dadurch nimmt die Volatilität ab, während gleichzeitig die Zentralenbanken durch verfehlte Geldpolitik das Vertrauen in das klassische Währungssystem nicht mehr aufrechterhalten können.[489] Alle potenziellen Anwendungsfelder der Blockchain werden in der Praxis implementiert und sind erfolgreich.[490] Welche Kryptowährungen sich dabei durchsetzen, entscheiden die Präferenzen der Konsumenten sowie die Lösungsansätze des Problems der langfristig konstanten Geldmenge.[491]

Eine Studie von Deloitte fügt diesen beiden Szenarien zwei weitere hinzu. In einem weiteren Extrem-Szenario können Kryptowährungen die Erwartungen nicht erfüllen und floppen. Hackingangriffe, sowie starke Kursschwankungen sorgen dafür, dass Investoren und Unternehmen sich zunehmend abwenden. Die Technologie kann nicht dem Wachstum entsprechend weiterentwickelt werden und fehlende Standards sorgen für einen Anstieg der kriminellen Nutzung. Kryptowährungen werden zwar weiterhin für Spekulationsgeschäfte genutzt, setzen sich aber auf unternehmerischer Ebene nicht durch.[492]

In einem weiteren Szenario, welches Deloitte skizziert, setzen sich große und finanzstarke Unternehmen durch, die sich bereits frühzeitig mit der Thematik auseinandergesetzt haben. Der dezentrale Gedanke rückt weiter in den Hintergrund, allerdings bieten Unternehmen komfortable und günstige Lösungen an, die auf der Blockchain-Technologie basieren. Viele Prozesse sind effizienter geworden. Finanzinstitute kooperieren miteinander und sorgen so für eine stetige Weiterentwicklung und gemeinsame Standards.[493]

---

488 Vgl. Hungerland et al. (2017), S. 64 f. (abgerufen am 07. Dez. 2018).

489 Vgl. Hungerland et al. (2017), S. 65 f. (abgerufen am 07. Dez. 2018).

490 Vgl. Deloitte B (o. D.) (abgerufen am 07. Dez. 2018).

491 Vgl. Hungerland et al. (2017), S. 65 f. (abgerufen am 07. Dez. 2018).

492 Vgl. Deloitte B (o. D.) (abgerufen am 07. Dez. 2018).

493 Vgl. Deloitte B (o. D.) (abgerufen am 07. Dez. 2018).

Darüber hinaus gibt es eine Vielzahl an weiteren Einschätzungen, in denen beispielsweise Bitcoins das Gold als Wertanlage ersetzen werden oder starke Regulierungen dafür sorgen, dass Kryptowährungen lediglich für Wenige sinnvoll anwendbar werden.

Nach ausführlicher Recherche und Erstellen dieser Thesis, schätze ich das Szenario der Nischenrolle derzeit am realistischsten ein. Dieses Szenario wird voraussichtlich mit dem Szenario der großen Unternehmen, die eine Vorreiterrolle einnehmen und eher zentralisierte Lösungen bieten, kombiniert. Kryptowährungen und Blockchain werden an Relevanz und Akzeptanz gewinnen, nicht aber das gesamte Währungssystem und dessen Intermediäre vollständig ablösen. Die beiden Extrem-Szenarien sind dabei gleichermaßen unwahrscheinlich. Zu einem ähnlichen Ergebnis kommt auch der Kryptoexperte Julian Hosp.[494] Trotz aller Vorbehalte geht der Trend weiter in Richtung Dezentralität, ohne dabei aber einen radikalen Umbruch zu verursachen. Hierbei wird sich herauskristallisieren, dass weder komplette Dezentralität noch alleinige Zentralisierung die Lösung ist. Bisher ist insbesondere der Zahlungsverkehr stark zentralisiert. Die derzeitige Dezentralisierung stellt ein Gegengewicht dar und wird für ein generelles Umdenken sorgen und neue Möglichkeiten eröffnen. Dabei gilt es, einen Mittelweg zu finden, der die Vorteile beider Systeme kombiniert. Wie genau der Mix aus zentralen und dezentralen Systemen aussieht, wird die Zukunft zeigen.

Die Handlungsempfehlungen für Unternehmen, die sich aus dem Eintreten des wahrscheinlichen Szenarios ergeben, betreffen insbesondere die Beobachtung der rechtlichen Entwicklung sowie Identifizierung der betroffenen Bereiche. Zudem ist es wichtig, Anwendungsfälle selbst zu erproben, da die notwendige Erfahrung nur durch eigenes Ausprobieren gewonnen werden kann. Dazu müssen intern Freiräume geschaffen werden. Darüber hinaus ist es empfehlenswert, die Standardisierung der Technologie weiter voran zu treiben, idealerweise in Kooperation mit anderen Unternehmen oder Organisationen. Dadurch ist zeitgleich auch eine aktive Gestaltung der Weiterentwicklung möglich.

[494] Vgl. Hosp B (2018), S. 244 f.

9 Zusammenfassende Schlussbetrachtung

Ziel der vorliegenden Thesis war es, die durch Kryptowährungen entstehenden Chancen und Risiken für Unternehmen zu identifizieren. Ausgehend von den Anfängen des Geldes wurde zunächst dargelegt, wie die weltweite Digitalisierung auch den Zahlungsverkehr beeinflusst und warum Kryptowährungen überhaupt entstanden sind. Anschließend wurden die technischen Aspekte der Blockchain ausführlich erläutert, da diese auch einen Einfluss auf die Chancen und Risiken haben. Es folgte eine Übersicht über den Bitcoin und über andere vielversprechende Altcoins, die aufgrund ihrer Eigenschaften viel praktisches Anwendungspotenzial bieten. Vor der Thematisierung der Chancen und Risiken wurden rechtliche Aspekte und mögliche Entwicklungsszenarien aufgezeigt, die derzeit in Verbindung mit Kryptowährungen diskutiert werden.

Im Rahmen dieser Masterthesis wurde eine umfangreiche Analyse der vorliegenden Literatur, diverser Artikel sowie von einigen Studien durchgeführt. Dabei wurde grundsätzlich festgestellt, dass es eine Vielzahl an Branchen gibt, denen enormes Potenzial für die Anwendung von Kryptowährungen und Blockchain zugesprochen wird. Es bestehen jedoch Unterschiede in der Akzeptanz und Nutzung einzelner Bereiche. Während der Finanzbranche und der Industrie großes Potenzial zur Anwendung zugesagt werden und diese bereits an praxistauglichen Umsetzungen arbeiten, eignen sich der öffentliche Sektor sowie Branchen mit einem hohen Maß an persönlichem Kontakt nur im geringen Maße für eine Implementierung. In vielen Bereichen tritt die Blockchain als innovativer Treiber hervor und nimmt eine Rolle als Plattform ein, die nicht nur zur Zahlungsabwicklung dient.

Derzeit ist die Nutzung von Kryptowährungen im Alltag auf einen kleinen Nutzerkreis beschränkt. Dies ist einerseits auf fehlende Akzeptanz zurückzuführen, andererseits auch auf rechtliche und technische Hürden. Die Berichterstattung über Kryptowährungen wird von mehrheitlich negativen Meldungen dominiert. Für Unternehmen herrscht noch Unklarheit darüber, welche Eigenschaften die eigenen Geschäftsmodelle aufweisen müssen, um von Kryptowährungen und Blockchain profitieren zu können. Zudem steht die Technologie noch am Anfang und somit sind viele Entwicklungen, beispielsweise der Einfluss durch staatliche Institutionen, noch nicht absehbar.

Auf der anderen Seite wurde festgestellt, dass immer mehr Unternehmen sich mit der Thematik beschäftigen und demnach die Relevanz von Kryptowährungen steigen wird.

In erster Linie werden davon aber Altcoins wie beispielsweise Ethereum, IOTA oder Ripple betroffen sein – der Bitcoin wird aller Voraussicht nach für Unternehmen zweitranging bleiben. Bei frühzeitiger Erkennung des Potenzials besteht die Chance, Wettbewerbsvorteile zu generieren und neue Marktsegmente zu erschließen. Darüber hinaus entstehen durch den Einsatz von Kryptowährungen Chancen zur Senkung der Kosten und Steigerung der Effizienz. Transaktionen können nahezu in Echtzeit abgewickelt und transparent sowie fälschungssicher auf der Blockchain hinterlegt werden. Smart Contracts können Prozesse automatisieren und Intermediäre in vielen Bereichen ersetzen.

Trotz des Hypes, berechtigt oder nicht, müssen Unternehmen sich in erster Linie fragen, ob Kryptowährungen und Blockchain überhaupt zum eigenen Geschäftsmodell passen und notwendige Grundlagen vorhanden sind. Zudem gibt es weiterhin Schwachstellen, die selbst Kryptowährungen und Blockchain nicht vermeiden können. Werden die falschen Produkte in den Container verladen, liefert auch die Blockchain falsche Ergebnisse. Schlechte Prozesse bleiben schlechte Prozesse – daher müssen die ersten Ansätze zur Implementierung auf der Organisationsebene stattfinden. Kryptowährungen sollten aus unternehmerischer Sicht ein strategisches Kernthema darstellen.

Auch die Frage danach, welche Kryptowährung zukünftig dominieren wird, kann nicht seriös beantwortet werden. Womöglich wird sich in erster Linie die Blockchain-Technologie oder das Tangle als innovativer Treiber durchsetzen – sicher ist lediglich, dass beides nicht mehr vollständig aus der Gesellschaft und der Wirtschaft verschwinden wird. Dabei werden häufig Vergleiche zu den Anfängen des Internets herangezogen. Anfänglich eine Revolution, der viele skeptisch gegenüberstanden, ist es heute längst zur Normalität geworden. In einigen Jahren zieht womöglich die Blockchain in den Alltag ein und sorgt für höhere Sicherheit, ohne dass dies bemerkbar ist.

Stand jetzt überwiegen die Risiken die Chancen oder bieten zumindest im Vergleich zu klassischen Zahlungsmitteln für den Verbraucher kaum einen wahrnehmbaren Vorteil. Für Unternehmen, aber auch für Verbraucher stellen Kryptowährungen und deren volatile Kurse im alltäglichen Online-Handel derzeit noch keine Alternative zur Bezahlung dar. Visa und PayPal wickeln Zahlungen schnell und zuverlässig ab und sind na-

hezu in alle Prozesse im Online-Handel integriert. Aus eigener Erfahrung kann festgehalten werden, dass IOTA-Tokens im Wert von 50 Euro nicht für einen Einkauf genutzt werden, wenn diese in einer Woche womöglich doppelt so viel wert sind. Zudem befinden sich viele angesprochene und weitere Blockchain-Projekte in einer Testphase und müssen ihre Alltagstauglichkeit in der Wirtschaft erst noch nachweisen.

Die Fragen nach der rechtlichen Regulierung und technischen Weiterentwicklung (beispielsweise Skalierbarkeit) nehmen in Hinblick auf die Zukunft zentrale Rollen ein. Danach wird sich entscheiden, wann, wie und ob sich eine Kryptowährung durchsetzt. Dies könnte je nach Branche unterschiedlich ausfallen – während Ethereum durch seine Smart Contracts Anwendungspotenziale im Alltag bietet, wird Ripple sich vermutlich eher als System im Bankensektor durchsetzen. Fast sicher ist, dass auch der Bitcoin, trotz seines Alters von fast zehn Jahren, die kommenden Jahre als Leitwährung weiterhin Relevanz auf den Kryptomärkten haben wird. Andererseits kann festgehalten werden, dass Altcoins und deren Blockchains, abseits der Kursspekulationen, zukünftig für eine massentaugliche Anwendung sorgen werden.

Wie dynamisch die gesamte Entwicklung rund um Kryptowährungen ist, zeigt sich daran, dass sich während des Verfassens dieser Arbeit neue technische Möglichkeiten ergeben haben, viele neue Kryptowährungen entstanden sowie Regulierungen in Kraft getreten sind. Von expliziten Handlungsempfehlungen für Branchen oder Unternehmen wird an dieser Stelle abgesehen, da zukünftige Entwicklungen weder abgeschätzt, noch allgemeingültige Lösungen für Unternehmen abgeleitet werden können. Da aber genereller Handlungsbedarf besteht, ergibt sich daraus eine Vielzahl an möglichen branchenspezifischen Forschungsmöglichkeiten. Spannende Forschungsfragen sind zudem, wie sich die derzeit diskutierten Chancen und Risiken in einigen Jahren entwickelt haben und welches Resümee hinsichtlich einer erfolgreichen Umsetzung gezogen werden kann. Viele Projekte mit Potenzial scheitern womöglich, woraus sich wiederum Ansätze für darauffolgende Projekte ergeben. Nur durch stetige Forschung lassen sich konkrete Empfehlungen für Unternehmen ableiten. Diese Arbeit soll eine Grundlage darstellen, die als Ausgangspunkt für weiterführende Forschungsfragen dient und vorab einen detaillierten Überblick über die Ist-Situation verschafft.

Insgesamt lässt sich der Schluss ziehen, dass Kryptowährungen generell deutliche Vorteile gegenüber herkömmlichen Zahlungsmitteln bieten. Für viele Risiken werden

zukünftig Lösungen gefunden und die innovative Blockchain-Technologie bietet noch weitaus mehr Möglichkeiten, als die bloße Zahlungsabwicklung. Die Entwicklung des Geldes ist auch immer eine Geschichte der Evolution. Bei jedem Erscheinen neuer Formen und Technologien gab es anfangs Vorbehalte, bis dann schlussendlich neue Zahlungssysteme entstanden. Kryptowährungen und Blockchain sind zwar im wirtschaftlichen Kontext noch ganz am Anfang, stellen aber diese nächste Stufe der Evolution dar. Wenn auch nicht klar ist, welche Kryptowährungen und Blockchain sich durchsetzen werden, die Idee dahinter ist gekommen, um dauerhaft zu bleiben und Einzug in den Alltag zu finden.

Literaturverzeichnis

Admiral Markets: „Was ist Ripple?“, o. D., URL: https://admiralmarkets.de/wissen/articles/forex-basics/was-ist-ripple (abgerufen am 17. Okt. 2018).

Atzler, Elisabeth: „Bei Sparkassen sind bald Überweisungen in Echtzeit möglich – aber selten gratis“, 2018, URL: https://www.handelsblatt.com/finanzen/banken-versicherungen/instant-payments-bei-sparkassen-sind-bald-ueberweisungen-in-echtzeit-moeglich-aber-selten-gratis/21246482.html (abgerufen am 07. Aug. 2018).

Badertscher, Marc: „Bitcoin explodiert - das sind jetzt die 8 Risiken“, 2016, URL: https://www.handelszeitung.ch/blogs/bits-coins/bitcoin-explodiert-das-sind-jetzt-die-8-risiken-1301885 (abgerufen am 17. Nov. 2018).

Barfuß, Karl Marten: Grundlagen der Geldtheorie, in: Geld und Währung (Hrsg. Barfuß, Karl Marten), Wiesbaden (Springer Gabler), 4. Auflage, 1992, S. 1 – 18.

Beckmann & Partner CONSULT: „Krypto-Währungen - eine Gefahr für Banken?“, 2018, URL: https://www.pressebox.de/pressemitteilung/beckmann-partner-consult-gmbh/Krypto-Waehrungen-eine-Gefahr-fuer-Banken/boxid/921257 (abgerufen am 03. Dez. 2018).

Bender, Markus: „Die neuen Generationen von Kryptowährungen lassen Bitcoin alt aussehen“, 2018, URL: https://www.focus.de/digital/experten/kryptowaehrungen-die-neuen-generationen-von-kryptowaehrungen-lassen-bitcoin-alt-aussehen_id_8896113.html (abgerufen am 04. Dez. 2018).

Berger, Carola F.: „Bitcoin Teil 2 – Bitcoin-Schürfen“, 2015, URL: https://www.cfb-translations.com/de/bitcoin-teil-2-bitcoin-schurfen/ (abgerufen am 22. Aug. 2018).

Bergmann, Christoph: „IOTA, die Kryptowährung für Maschinen: eine Blockchain ohne Blöcke“, 2016, URL: https://bitcoinblog.de/2016/07/13/iota-die-krypto-waehrung-fuer-maschinen-eine-blockchain-ohne-bloecke/ (abgerufen am 23. Okt. 2018).

Bergmann, Christoph: „ICOs und die Regulierer: Eine Übersicht“, 2017, URL: https://bitcoinblog.de/2017/10/06/icos-und-die-regulierer-eine-uebersicht/ (abgerufen am 13. Nov. 2018).

Berschens, Ruth: „EU erwägt striktere Regeln für Bitcoin & Co.“, 2018, URL: https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/kryptowaehrungen-eu-erwaegt-striktere-regeln-fuer-bitcoin-und-co-/22993608.html?ticket=ST-388296-6x3SZ6ZnU4LENiGEVeig-ap1 (abgerufen am 13. Nov. 2018).

Beutelspacher, Albrecht; Neumann, Heike B.; Schwarzpaul, Thomas: Kryptografie in Theorie und Praxis – Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld, Wiesbaden (Vieweg+Teubner), 2. Auflage, 2010.

Binder, Evelyn; Geisler, Hendrik; Schmidt, Björn: „Experte erklärt Bitcoin-Hype: „Alle Leute wollen einsteigen, daher steigt der Kurs““, 2017, URL: https://www.berliner-zeitung.de/wirtschaft/experte-erklaert-bitcoin-hype--alle-leute-wollen-einsteigen--daher-steigt-der-kurs--29024516 (abgerufen am 18. Nov. 2018).

Bitcoin: „Wie funktioniert Bitcoin?“, o. D., URL: https://bitcoin.org/de/wie-es-funktioniert (abgerufen am 27. Aug. 2018).

Bitcoin-Generator: „Die Vorteile von Kryptowährungen“, o. D., URL: https://bitcoin-generator.de/vorteile-kryptowaehrungen (abgerufen am 30. Nov. 2018).

Bitcoinmag A: „Kryptowährung kaufen: Alles was Sie für Ihr Investment wissen müssen!“, o. D., URL: https://www.bitcoinmag.de/investment/kryptowaehrung-kaufen/a-117 (abgerufen am 25. Okt. 2018).

Bitcoinmag B: „Mit Kryptowährungen handeln – Der ultimative Anfänger-Guide!“, o. D., URL: https://www.bitcoinmag.de/investment/kryptowaehrung-handeln (abgerufen am 24. Okt. 2018).

Bitcoinmining: „Erste Schritte“, o. D., URL: https://www.bitcoinmining.com/de/ (abgerufen am 18. Sept. 2018).

Bitcoinwisdom: „Bitcoin Difficulty“, o. D., URL: https://bitcoinwisdom.com/bitcoin/difficulty (abgerufen am 18. Sept. 2018).

Blockchain A: „Blockchain Size“, o. D., URL: https://www.blockchain.com/de/charts/blocks-size (abgerufen am 20. Nov. 2018).

Blockchain B: „Difficulty“, o. D., URL: https://www.blockchain.com/de/charts/difficulty?timespan=all (abgerufen am 18. Sept. 2018).

Blockchain C: „Hashrate Verteilung“, o. D., URL: https://www.blockchain.com/de/pools (abgerufen am 27. Nov. 2018).

Blockchain: „Größte Transaktionen“, 2018, URL: https://www.blockchain.com/de/btc/largest-recent-transactions (abgerufen am 20. Aug. 2018).

Blockchain-Nachrichten: „Hash“, 2016, URL: http://blockchain-nachrichten.com/blockchaintechnologien/hash# (abgerufen am 11. Sept. 2018).

Blockchainwelt A: „Genesis Block | Anfang einer Kryptowährung“, 2018, URL: https://blockchainwelt.de/genesis-block-bitcoin-ethereum-blockchain-kryptowaehrung/ (abgerufen am 16. Aug. 2018).

Blockchainwelt B: „Bitcoin Mining | Alles was Sie wissen müssen“, 2018, URL: https://blockchainwelt.de/bitcoin-mining-alles-was-sie-wissen-muessen/ (abgerufen am 22. Sept. 2018).

Blockchainwelt C: „Distributed Ledger Technologie (DLT) ist mehr als Blockchain“, 2018, URL: https://blockchainwelt.de/dlt-distributed-ledger-technologie-ist-mehr-als-blockchain/ (abgerufen am 29. Nov. 2018).

Blockchainwelt D: „Die Rolle der Kryptographie innerhalb der Blockchain-Technologie“, 2018, URL: https://blockchainwelt.de/kryptographie-innerhalb-der-blockchain-technologie/ (abgerufen am 15. Sept. 2018).

BlockLAB: „Skalieren Blockchains? Sorgen und Lösungsansätze“, 2017, URL: https://site.blocklab.de/2017/Skalierung/ (abgerufen am 20. Nov. 2018).

Brandt, Mathias: „Internet of Things wird bis 2020 alltäglich“, 2014, URL: https://de.statista.com/infografik/2937/mit-dem-internet-of-things-verbundenen-geraete/ (abgerufen am 21. Okt. 2018).

Brandt, Mathias: „Anleger investieren Milliarden in neue Krypto-Coins“, 2018, URL: https://de.statista.com/infografik/11517/volumen-von-ico-finanzierungsrunden-pro-monat/ (abgerufen am 29. Okt. 2018).

Brenneis, Friedemann: „Kryptowährungen: Chancen, Risiken und neue Anwendungsfelder – Interview mit Friedemann Brenneis“, 2017, URL: https://veranstaltungen.handelsblatt.com/bankengipfel/kryptowaehrungen-chancen-risiken-und-neue-anwendungsfelder-interview-mit-friedemann-brenneis/ (abgerufen am 29. Nov. 2018).

BTC-Echo A: „Was ist Proof-of-Work?“, o. D., URL: https://www.btc-echo.de/tutorial/was-ist-proof-of-work-wie-funktioniert-konsens-mechanismus/ (abgerufen am 28. Aug. 2018).

BTC-Echo B: „Was ist Proof-of-Stake?“, o. D., URL: https://www.btc-echo.de/tutorial/was-ist-proof-of-stake/ (abgerufen am 22. Nov. 2018).

BTC-Echo C: „Was ist eine Sidechain?“, o. D., URL: https://www.btc-echo.de/tutorial/was-ist-eine-sidechain/ (abgerufen am 09. Sept. 2018).

BTC-Echo D: „Was ist Ethereum (ETH)?“, o. D., URL: https://www.btc-echo.de/tutorial/was-ist-ethereum-ether/ (abgerufen am 04. Dez. 2018).

BTC-Echo E: „Wie funktioniert Ether-Mining?“, o. D., URL: https://www.btc-echo.de/tutorial/wie-funktioniert-ethereum-mining/ (abgerufen am 10. Okt. 2018).

BTC-Echo F: „Was ist Ripple?“, o. D., URL: https://www.btc-echo.de/was-ist-ripple/ (abgerufen am 17. Okt. 2018).

BTC-Echo G: „Was ist eine 51%-Attacke und wie funktioniert sie?“, o. D., URL: https://www.btc-echo.de/tutorial/bitcoin-51-attacke/ (abgerufen am 27. Nov. 2018).

Bücker, Till: „ICOs sind tot - es lebe der STO!“, 2018, URL: https://boerse.ard.de/anlageformen/kryptowaehrungen/stos-probleme-der-icos-geloest100.html (abgerufen am 31. Okt. 2018).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): „Virtuelle Währungen/Virtual Currency (VC)“, o. D., URL: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html (abgerufen am 04. Nov. 2018).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): „Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs)“, 2017, URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html (abgerufen am 30. Okt. 2018).

Bundesministerium der Finanzen: „Umsatzsteuerliche Behandlung von Bitcoin und anderen sog. virtuellen Währungen“, 2018, URL: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.pdf?__blob=publicationFile&v=1 (abgerufen am 06. Nov. 2018).

Bundesregierung: „Wie lange dauert ein Asylverfahren?“, o. D., URL: https://www.bundesregierung.de/Content/DE/Lexikon/FAQ-Fluechtlings-Asylpolitik/1-was-muss-ich-ueber-fluechtlinge-wissen/430-Dauer-Asylverfahren.html (abgerufen am 06 Dez. 2018).

Business Insider Deutschland: „Überraschende Studie: So beliebt ist die Kryptowährung Bitcoin in Deutschland wirklich“, 2018, URL: https://www.businessinsider.de/ueberraschende-studie-so-beliebt-ist-die-kryptowaehrung-bitcoin-in-deutschland-wirklich-2018-2 (abgerufen am 17. Nov. 2018).

Capital Group: „Capital Group: Blockchain - Revolution auf dem Finanzmarkt“, 2018, URL: https://www.fundresearch.de/blockchain/capital-group-blockchain-revolution-auf-dem-finanzmarkt-23751.php (abgerufen am 05. Dez. 2018).

CLLB Rechtsanwälte: „Überblick über die aufsichtsrechtlichen Regelungen für ICOs, TGEs und Cryptocurrencies weltweit“, o. D., URL: https://www.anwalt.de/rechtstipps/ueberblick-ueber-die-aufsichtsrechtlichen-regelungen-fuer-icos-tges-und-cryptocurrencies-weltweit_131590.html (abgerufen am 13. Nov. 2018).

CoinMarketCap A: „Top 100 Kryptowährungen nach Börsenwert“, o. D., URL: https://coinmarketcap.com/de/ (abgerufen am 20. Nov. 2018).

CoinMarketCap B: „Charts zu Bitcoin“, o. D., URL: https://coinmarketcap.com/de/currencies/bitcoin/#charts (abgerufen am 13. Okt. 2018).

CoinMarketCap C: „Charts zu Ethereum“, o. D., URL: https://coinmarketcap.com/de/currencies/ethereum/#charts (abgerufen am 13. Aug. 2018).

CoinMarketCap D: „Charts zu XRP“, o. D., URL: https://coinmarketcap.com/de/currencies/ripple/#charts (abgerufen am 17. Okt. 2018).

CoinMarketCap E: „Charts zu IOTA“, o. D., URL: https://coinmarketcap.com/de/currencies/iota/#charts (abgerufen am 21. Okt. 2018).

Cointrend: „Was bedeutet Market Cap im Zusammenhang mit Kryptowährungen?“, 2017, URL: https://cointrend.de/kryptowiki/market-cap/ (abgerufen am 13. Aug. 2018).

Crypto Magazin: „Proof of Importance (POI)“, o. D., URL: https://www.crypto-magazin.com/proof-of-importance-poi/ (abgerufen am 01. Sept. 2018).

Crypto Magazin: „Das Vertrauen in Kryptowährungen sinkt“, 2018, URL: https://www.crypto-magazin.com/das-vertrauen-in-kryptowaehrungen-sinkt-1321314/ (abgerufen am 07. Aug. 2018).

Cryptolist A: „Was ist Ripple?“, o. D., URL: https://www.cryptolist.de/ripple (abgerufen am 17. Okt. 2018).

Cryptolist B: „Was ist IOTA?“, o. D., URL: https://www.cryptolist.de/iota (abgerufen am 23. Okt. 2018).

Cryptowolf: „Was ist IOTA?“, 2018, URL: https://cryptowolf.de/was-ist-iota/ (abgerufen am 23. Okt. 2018).

Dannenberg, Marius; Ulrich, Anja: E-Payment und E-Billing – Elektronische Bezahlsysteme für Mobilfunk und Internet, Wiesbaden (Gabler/GWV Fachverlage GmbH), 2004.

Decentralbox: „Was ist eine Blockchain?“, 2017, URL: https://decentralbox.com/was-ist-eine-blockchain/ (abgerufen am 29. Nov. 2018).

Deloitte A: „Die Blockchain aus Sicht des Datenschutzrechts – Eine kurze Einführung zu datenschutzrechtlichen Implikationen“, o. D., URL: https://www2.deloitte.com/dl/de/pages/legal/articles/blockchain-datenschutzrecht.html (abgerufen am 03. Nov. 2018).

Deloitte B: „Blockchain – ein Game-Changer?“, o. D., URL: https://www2.deloitte.com/de/de/pages/innovation/contents/Blockchain-Game-Changer.html (abgerufen am 07. Dez. 2018).

Deutsche Bundesbank: „Begriff und Aufgaben des Geldes – Erscheinungsformen des Geldes im Wandel der Zeit“, o. D., https://www.bundesbank.de/de/service/schule-und-bildung/schuelerbuch-geld-und-geldpolitik-digital/erscheinungsformen-des-geldes-im-wandel-der-zeit-614064 (abgerufen am 11. Jul. 2018).

Deutsche Bundesbank: „Zahlungsverkehr im Wandel – Was sind die Herausforderungen?“, 2017, URL: https://www.bundesbank.de/de/presse/reden/zahlungsverkehr-im-wandel---was-sind-die-herausforderungen--711098 (abgerufen am 07. Aug. 2018).

Deutsche Bundesbank: „Bargeld bleibt das beliebteste Zahlungsmittel“, 2018, URL: https://www.bundesbank.de/de/aufgaben/themen/bargeld-bleibt-das-beliebteste-zahlungsmittel-665636 (abgerufen am 17. Nov. 2018).

Diemers, Daniel et al.: „Initial Coin Offerings – Eine strategische Perspektive“, 2018, URL: https://www.pwc.ch/de/publications/2018/20180628_PwC%20S&%20CVA%20ICO%20Report_DE.pdf (abgerufen am 31. Okt. 2018).

Duisberg, Alexander: „Blockchain und Smart Contracts – Rechtsfragen einer digitalen Schlüsseltechnologie“, 2017, URL: https://digitaleweltmagazin.de/2017/07/18/blockchain-und-smart-contracts-rechtsfragen-einer-digitalen-schluesseltechnologie/ (abgerufen am 05. Nov. 2018).

Eatough, Jenna: „Rechtliche Unsicherheiten bei Blockchains und Smart Contracts“, 2017, URL: https://www.btc-echo.de/rechtliche-unsicherheiten-bei-blockchains-und-smart-contracts/ (abgerufen am 05. Nov. 2018).

Eberle, Andre: „Strengere Regulierungen durch EU im September“, 2018, URL: https://coincierge.de/2018/strengere-regulierungen-durch-eu-im-september/ (abgerufen am 13. Nov. 2018).

Eberle, Patrick: „Regulierung der Kryptowährungen schreitet in Japan voran“, 2018, URL: https://coincierge.de/2018/regulierung-der-kryptowaehrungen-schreitet-in-japan-voran/ (abgerufen am 13. Nov. 2018).

Ehrlicher, Werner: Geldtheorie und Geldpolitik (III): Geldtheorie, in: Handbuch der Wirtschaftswissenschaft (HdWW) (Hrsg.: Albers, Willi et al.), Stuttgart, New York, Tübingen, Göttingen, Zürich (Gustav Fischer, J.C.B.Mohr, Vandenhoeck & Ruprecht), 3. Band, 1982, S. 374 – 391.

Eibl, Maximilian; Gaedke, Martin (Hrsg.): „Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung“, 2017, URL: https://dl.gi.de/bitstream/handle/20.500.12116/3865/B13-1.pdf?sequence=1&isAllowed=y (abgerufen am 03. Nov. 2018).

Ellrich, Mirko: „Geographie Infothek – Infoblatt Die Geschichte des Geldes“, 2012, URL: https://www2.klett.de/sixcms/list.php?page=infothek_artikel&extra=Wirtschaftskunde-Online&artikel_id=93622&inhalt=klett71prod_1.c.172156.de (abgerufen am 11. Jul. 2018).

Erle, Christoph: „4 Blockchain Anwendungsfälle im Finanzbereich“, 2017, URL: https://www.management-circle.de/blog/4-blockchain-anwendungsfaelle-im-finanzbereich/ (abgerufen am 05. Dez. 2018).

Ernst, Rob: „Ethereum vs. Bitcoin: Aktueller Vergleich von ETH & BTC“, 2018, URL: https://blockchain-hero.com/ethereum-vs-bitcoin/ (abgerufen am 20. Nov. 2018).

Feil, Thomas: „Bitcoin und Kryptowährungen rechtlich!“, 2018, URL: https://www.recht-freundlich.de/bitcoin-kryptowaehrungen/bitcoin-kryptowaehrungen-rechtlich#Zivilrechtliche_Betrachtungsweise (abgerufen am 04. Nov. 2018).

Filbinger, Konstantin: „Chancen und Risiken für Unternehmen, die Kryptowährungen für Zahlungen akzeptieren“, 2018, URL: https://www.haufe.de/compliance/management-praxis/vorteile-und-risiken-wenn-unternehmen-kryptowaehrung-akzeptieren_230130_445568.html (abgerufen am 02. Dez. 2018).

Finanzfluss: „Ripple (XRP) einfach erklärt!“, o. D., URL: https://www.finanzfluss.de/was-ist-ripple/ (abgerufen am 17. Okt. 2018).

Finanzgeflüster: „Bitcoin Fork und das Steuerrecht (Das musst du wissen!)“, 2017, URL: https://www.finanzgefluester.de/bitcoin-fork-und-das-steuerrecht/ (abgerufen am 06. Nov. 2018).

Frankfurter Allgemeine Zeitung (FAZ): „Chaostage bei Bitcoin“, 2017, URL: http://www.faz.net/aktuell/finanzen/finanzmarkt/bitcoin-kursstuerze-befeuern-skepsis-gegenueber-kryptowaehrung-15290470.html (abgerufen am 07. Aug. 2018).

Frankfurter Allgemeine Zeitung A (FAZ): „Die Deutschen hängen an Münzen und Scheinen“, 2018, URL: http://www.faz.net/aktuell/finanzen/deutsche-lieben-bargeld-15448237.html (abgerufen am 19. Jul. 2018).

Frankfurter Allgemeine Zeitung B (FAZ): „Stromverbrauch von Bitcoin steigt schneller als erwartet“, 2018, URL: http://www.faz.net/aktuell/finanzen/digital-bezahlen/bitcoin-stromverbauch-bei-herstellung-enorm-hoch-15876893.html (abgerufen am 22. Nov. 2018).

Fridgen, Gilbert: Blockchain – Eine revolutionäre Idee und ihr reelles Potenzial, Vortrag bei der OTTO GmbH & Co KG, Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT, 19. Sept. 2018.

Fried: „The History of Bitcoin In Pictures“, o. D., URL: https://fried.com/history-of-bitcoin/ (abgerufen am 13. Okt. 2018).

Fuster, Thomas: „Bitcoin ist in Venezuela zur wichtigsten Parallelwährung aufgestiegen“, 2017, URL: https://www.nzz.ch/wirtschaft/kryptowaehrungen-notwehr-gegen-den-staat-ld.1305160 (abgerufen am 30. Nov. 2018).

Gabler Wirtschaftslexikon: „Definition Geld“, 2018, URL: https://wirtschaftslexikon.gabler.de/definition/geld-32540/version-256083 (abgerufen am 10. Jul. 2018).

Giese, Philipp: „Lightning-Network führt Transaktionen zwischen verschiedenen Blockchains durch“, 2017, URL: https://www.btc-echo.de/lightning-network-fuehrt-transaktionen-zwischen-verschiedenen-blockchains-durch/ (abgerufen am 19. Nov. 2018).

Giese, Philipp: „Was ist das Bitcoin Lightning Network?“, 2018, URL: https://www.btc-echo.de/was-ist-das-bitcoin-lightning-network/ (abgerufen am 20. Nov. 2018).

Giese, Philipp et al.: Die Bitcoin-Bibel – Das Buch zur digitalen Währung, Kleve (BTC-ECHO), 2. Auflage, 2017.

Giese, Tanja: „Erste bankgestützte Kryptobörse der Welt eröffnet in Japan“, 2018, URL: https://www.btc-echo.de/erste-bankgestuetzte-kryptoboerse-der-welt-eroeffnet-in-japan/ (abgerufen am 27. Okt. 2018).

Glücklich, Alexander A: Blockchain für Anfänger – Alles was du über Blockchain, Bitcoin, Smart Contracts und Kryptowährung wissen musst (Selberverlag), 2017.

Glücklich, Alexander B: Ethereum für Anfänger – Was ist Ethereum? Was du über die Kryptowährung Ether, die Ethereum Blockchain, Smart Contracts, dApps, und Ethereum Mining wissen musst und wie du investieren kannst (Selbstverlag), 2017.

Gogniat, Yves: „Die Blockchain – ein rechtliches Minenfeld?“, 2018, URL: https://morethandigital.info/die-blockchain-ein-rechtliches-minenfeld/ (abgerufen am 05. Nov. 2018).

Gojdka, Victor: „Warum Bitcoin gerade so abrauscht“, 2018, URL: https://www.sueddeutsche.de/digital/bitcoin-kursverlust-1.4220711 (abgerufen am 24. Nov. 2018).

Göß, Simon: „E-Mobility und die Blockchain: Das „Car eWallet““, 2017, URL: https://blog.energybrainpool.com/e-mobility-und-die-blockchain-das-car-ewallet/ (abgerufen am 06. Dez. 2018).

Grinschuk, Eugen: Blockchain – Ein neuer GameChanger: Blockchain Grundlagen & Blockchain für Anfänger – Die Blockchain Technologie erklärt (Selbstverlag), 2017.

Gründerszene: „Disruption“, URL: https://www.gruenderszene.de/lexikon/begriffe/disruption?interstitial_click (abgerufen am 03. Dez. 2018).

Grusch, Alfred; Melingo, Diego: Handbuch der Edelmetall-Veranlagungen: Warum Gold, Silber und Platin ein fixer Bestandteil Ihres Vermögens sein sollten, Wien (Linde Verlag), 2012.

Hahn, Christopher; Wons, Adrian: Initial Coin Offering (ICO) – Unternehmensfinanzierung auf Basis der Blockchain-Technologie, Wiesbaden (Springer Gabler), 2018.

Harms, Andreas: „So viel Strom frisst das Bitcoin-System“, 2018, URL: https://www.dasinvestment.com/studie-enthuellt-so-viel-strom-frisst-das-bitcoin-system/ (abgerufen am 21. Nov. 2018).

Heckmann, Dirk; Schmid, Alexander: „Studie: Blockchain und Smart Contracts – Recht und Technik im Überblick“, 2017, URL: https://vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Planung-und-Koordination/2017/Downloads/2017-09-12-NH-vbw-Blockchain-und-Smart-Contracts_ChV-Fu%C3%9Fnoten.pdf (abgerufen am 05. Nov. 2018).

Hellinger, Axel: „Smart Contract | Wirksamkeit & Unwirksamkeit von Vertragsprogrammen“, 2016, URL: https://hellinger.legal/smart-contract/ (abgerufen am 05. Nov. 2018).

Herzog, Cornelius; Oest, Philipp: „Blockchains in der Supply Chain - “Edi-on-dope” oder viel mehr?“, 2017, URL: https://www.oliverwyman.de/our-expertise/insights/2017/nov/blockchains-in-der-supply-chain.html (abgerufen am 04. Dez. 2018).

Heun, Volker: Bitcoin & Co – Eine neue Weltwährung: Chancen und Risiken für Investoren, Norderstedt (BOD – Books on Demand), 2018.

Hileman, Garrick: „Most countries in the ’10 most likely’ to adopt bitcoin are in the developing world“, 2016, URL: http://blogs.lse.ac.uk/businessreview/2016/05/12/most-countries-in-the-10-most-likely-to-adopt-bitcoin-are-in-the-developing-world/ (abgerufen am 30. Nov. 2018).

Hilmes, Christian: „Mehrheit der Deutschen sieht Bitcoin & Co kritisch“, 2018, URL: https://www.dasinvestment.com/umfrage-zu-kryptowaehrungen-mehrheit-der-deutschen-sieht-bitcoin--co-kritisch/ (abgerufen am 18. Nov. 2018).

Honig, Raphael: „Bitcoin Difficulty – Der Schwierigkeitsgrad beim Mining“, 2018, URL: https://www.kryptopedia.org/bitcoin-difficulty-der-schwierigkeitsgrad-beim-mining/ (abgerufen am 18. Sept. 2018).

Horch, Phillip A: „Der Preis der Dezentralität – Blockchain und Skalierbarkeit“, 2018, URL: https://www.btc-echo.de/der-preis-der-dezentralitaet-blockchain-und-skalierbarkeit/ (abgerufen am 19. Nov. 2018).

Horch, Phillip B: „Bitcoin, die Umweltkatastrophe? Was gesagt werden muss“, 2018, URL: https://www.btc-echo.de/bitcoin-die-umweltkatastrophe-was-gesagt-werden-muss/ (abgerufen am 22. Nov. 2018).

Hosp, Julian: Kryptowährungen – Bitcoin, Ethereum, Blockchain, ICO’s & Co. einfach erklärt (Verlag Julian Hosp Coaching LTD), 2017.

Hosp, Julian: „Wie gut eignen sich Kryptowährungen für illegale Aktivitäten?“, 2018, URL: https://www.btc-echo.de/wie-gut-sind-kryptowaehrungen-fuer-illegale-aktivitaeten/ (abgerufen am 01. Dez. 2018).

Hosp, Julian A: Kryptowährungen – Bitcoin, Ethereum, Blockchain, ICO’s & Co. einfach erklärt (Verlag Julian Hosp Coaching LTD), 2018.

Hosp, Julian B: Blockchain 2.0: Einfach erklärt – weit mehr als nur Bitcoin (Verlag Julian Hosp Coaching LTD), 2018.

Huber, Florian: „Startup-Finanzierung mit ICOs: Zu gut, um wahr zu sein?“, o. D., URL: https://www.deutsche-startups.de/2018/02/12/startup-finanzierung-mit-icos-zu-gut-um-wahr-zu-sein/ (abgerufen am 31. Okt. 2018).

Hungerland, Fabian et al.: „Die Zukunft des Geldes – Das Geld der Zukunft“, 2017, URL: https://www.berenberg.de/files/Berenberg/Publikationen/Studie_Strategie_2030/Berenberg-HWWI%20Studie_Die%20Zukunft%20des%20Geldes%20-%20Das%20Geld%20der%20Zukunft.pdf (abgerufen am 07. Dez. 2018).

IBM: „Blockchain für Supply Chain“, o. D., URL: https://www.ibm.com/blockchain/de-de/supply-chain/ (abgerufen am 04. Dez. 2018).

IOTA Support: „Eine Einleitung zu IOTA“, o. D., URL: https://iotasupport.com/whatisiota_de.shtml (abgerufen am 20. Okt. 2018).

IT Finanzmagazin: „Bezahlen per Kryptowährung? UTrust will die Vorzüge von PayPal mit DLT verbinden – das CEO-Interview“, o. D., URL: https://www.it-finanzmagazin.de/bezahlen-kryptowaehrungen-utrust-paypal-dlt-ceo-interview-70679/ (abgerufen am 06. Dez. 2018).

Kalt, Benjamin: „Wie sicher sind die beliebtesten Zahlungsmittel online?“, 2018, URL: https://www.trustedshops.de/blog/die-beliebtesten-zahlungsmittel-online/ (abgerufen am 01. Aug. 2018).

Kaulartz, Markus: „Mogelpackung oder Megatrend: Kryptowährungen auf dem Vormarsch“, o. D., URL: https://www.deutscheranwaltspiegel.de/mogelpackung-oder-megatrend-kryptowaehrungen-auf-dem-vormarsch/ (abgerufen am 04. Nov. 2018).

Kerscher, Daniel: Handbuch der digitalen Währungen – Bitcoin, Litecoin und 150 weitere Kryptowährungen im Überblick, Dingolfing (Kemacon UG), 2014.

Kilic, Klemens: „Warum der Wert von Kryptowährungen so stark schwankt“, 2018, URL: https://www.wired.de/collection/business/woher-kommt-die-volatilitaet-von-kryptowaehrungen (abgerufen am 24. Nov. 2018).

Koenig, Aaron: Crypto Coins – Investieren in digitale Währungen, München (Finanz-Buch Verlag), 2017.

Kreditkarten: „Kryptowährungen“, o. D., URL: https://www.kreditkarte.net/krypto-waehrungen/#risiken (abgerufen am 25. Nov. 2018).

Krempl, Stefan: „Geldwäsche: EU-Parlament beschließt schärfere Regeln für Kryptowährungen und Vorratsspeicherung von Finanzdaten“, 2018, URL: https://www.heise.de/newsticker/meldung/Geldwaesche-EU-Parlament-beschliesst-schaerfere-Regeln-fuer-Kryptowaehrungen-und-Vorratsspeicherung-4027647.html (abgerufen am 13. Nov. 2018).

Kröner, Andreas: „Europäische Regelungen für Kryptosparpläne sind realitätsfern“, 2018, URL: https://www.handelsblatt.com/meinung/kommentare/kommentar-europaeische-regelungen-fuer-kryptosparplaene-sind-realitaets-fern/22917120.html (abgerufen am 13. Nov. 2018).

Kryptomagazin: „Bitcoin – Vorteile für Unternehmen“, o. D., URL: https://www.krypto-magazin.de/bitcoin-vorteile-fuer-unternehmen/ (abgerufen am 02. Dez. 2018).

Kryptoszene: „Ripple“, o. D., URL: https://kryptoszene.de/kryptowaehrungen/ripple/ (abgerufen am 17. Okt. 2018).

Lackes, Richard: „Internet der Dinge“, o. D., URL: https://wirtschaftslexikon.gabler.de/definition/internet-der-dinge-53187 (abgerufen am 21. Okt. 2018).

Lang, Mirco; Augsten, Stephan: „Was ist überhaupt ein Block?“, 2017, URL: https://www.dev-insider.de/was-ist-ueberhaupt-ein-block-a-638193/ (abgerufen am 25. Aug. 2018).

Lange, Guido A: „Plant China eine eigene Kryptowährung?“, 2018, URL: https://kryptoszene.de/news/plant-china-eine-eigene-kryptowaehrung/ (abgerufen am 12. Nov. 2018).

Lange, Guide B: „Bitcoin Mining verursacht im Jahr soviel CO2 wie 1 Million Transatlantik Flüge“, 2018, URL: https://kryptoszene.de/news/bitcoin-mining-verursacht-im-jahr-so-viel-co2-wie-1-million-transatlantik-fluege/ (abgerufen am 22. Nov. 2018).

Ley, Alina: Erfolgsfaktoren von Kryptowährungen: Wie Unternehmen die elektronische Zahlungsmethode effizienzsteigernd nutzen können, (Studylab), 2017.

Mago, Felix; Gillen Tobias (Hrsg.): Das Bitcoin-Handbuch – Bitcoin von A bis Z, Hannover (jmb-Verlag), 2016.

Marshall, Andrew: „Bitcoin-Skalierungsproblem, Erklärt“, 2018, URL: https://de.cointelegraph.com/explained/bitcoin-scaling-problem-explained (abgerufen am 20. Nov. 2018).

Meyer, Jan Heinrich: „Digital Cash – Aus der Nische in den Mainstream: Kryptowährungen als disruptive Kraft im Finanzsystem“, 2018, URL: https://www.der-bank-blog.de/digital-cash-mainstream/mobile-payment/34382/ (abgerufen am 18. Nov. 2018).

Misiak, Marcus: „Bitcoin Cash Hard Fork ist aktiviert – Bitcoin Cash ABC vs. BCH SV“, 2018, URL: https://coin-hero.de/bitcoin-cash-hard-fork-ist-aktiviert-bitcoin-cash-abc-vs-bch-sv/ (abgerufen am 20. Nov. 2018).

Mühlbauer, Peter: „Iran gibt weitere Details zu seiner neuen Kryptowährung bekannt“, 2018, URL: https://www.heise.de/tp/features/Iran-gibt-weitere-Details-zu-seiner-neuen-Kryptowaehrung-bekannt-4150579.html (abgerufen am 02. Sept. 2018).

Nakamoto, Satoshi; „Bitcoin: A Peer-to-Peer Electronic Cash System“, o. D., URL: https://bitcoin.org/bitcoin.pdf (abgerufen am 13. Okt. 2018).

Neumann, Daniel: „Über 1.600 Bitcoin Geldautomaten für Argentinien in Planung“, 2018, URL: https://coin-update.de/ueber-1-600-bitcoin-geldautomaten-fuer-argentinien-in-planung/ (abgerufen am 12. Nov. 2018).

Neumann, Susanne; Demidova, Ekaterina; Kohlhoff, Mareike: „Potenziale der Blockchain in der Energiewirtschaft“, 2017, URL: https://www.exxeta.com/fileadmin/Exxeta/Documents/Publikationen/2017-03_ew_Potenziale_der_Blockchain.pdf (abgerufen am 06. Dez. 2018).

New Alchemy: „A short history of smart contract hacks on Ethereum“, 2018, URL: https://medium.com/new-alchemy/a-short-history-of-smart-contract-hacks-on-ethereum-1a30020b5fd (abgerufen am 27. Nov. 2018).

Niedermeier, Stephan: „Die Geschichte von Ethereum“, 2017, URL: https://eth-blog.de/geschichte-von-ethereum/ (abgerufen am 15. Okt. 2018).

Obertreis, Rolf: „Fjordwasser für grüne Bitcoins“, 2018, URL: https://www.tagesspiegel.de/wirtschaft/kryptowaehrung-fjordwasser-fuer-gruene-bitcoins/22824622.html (abgerufen am 22. Nov. 2018).

Orcutt, Mike: „Schlaue Verträge voller Lücken“, 2018, URL: https://www.heise.de/tr/artikel/Schlaue-Vertraege-voller-Luecken-3986434.html (abgerufen am 27. Nov. 2018).

Ostler, Ulrike A: „Tradelens von Maersk und IBM soll das Schifffahrtsökosystem umkempeln“, 2018, URL: https://www.datacenter-insider.de/tradelens-von-maersk-und-ibm-soll-das-schifffahrtsoekosystem-umkempeln-a-741365/ (abgerufen am 29. Sept. 2018).

Ostler, Ulrike B: „Maersk und IBM formen ein Joint Venture für Blockchain“, 2018, URL: https://www.datacenter-insider.de/maersk-und-ibm-formen-ein-joint-venture-fuer-blockchain-a-677400/ (abgerufen am 29. Sept. 2018).

Özel, Yunus: „Skalierbarkeit ist die Priorität der Entwicklungsteams von Kryptowährungen“, o. D., URL: https://de.decentral.news/skalierbarkeit-ist-die-prioritat-der-entwicklungsteams-von-kryptowahrungen/ (abgerufen am 20. Nov. 2018).

Passwort-Generator: „Kryptowährung: Das Bargeld der Zukunft?“, o. D., URL: https://www.passwort-generator.com/kryptowaehrung/#pseudonymitaet-statt-anonymitaet (abgerufen am 01. Dez. 2018).

PayPal A: „Über PayPal“, o. D., URL: https://www.paypal.com/de/webapps/mpp/about (abgerufen am 02. Aug. 2018).

PayPal B: „Käuferschutz“, o. D., URL: https://www.paypal.com/de/webapps/mpp/paypal-safety-and-security (abgerufen am 02. Aug. 2018).

Perlaki, Dominik: „Bitcoin: 8 Probleme der bekanntesten Kryptowährung“, 2017, URL: https://www.derbrutkasten.com/bitcoin-8-nachteile-der-bekanntesten-kryptowaehrung/ (abgerufen am 22. Nov. 2018).

Peter, Viktor et al: „Blockchain in der Energiewirtschaft – Potenziale für Energieversorger“, 2017, URL: https://www.bdew.de/media/documents/BDEW_Blockchain_Energiewirtschaft_10_2017.pdf (abgerufen am 06. Dez. 2018).

Peters, Rene: „Was ist Hashing? Unter der Haube der Blockchain“, 2017, URL: https://kryptozeitung.com/was-ist-hashing-blockchain/ (abgerufen am 15. Sept. 2018).

Pielke, Walther: Besteuerung von Kryptowährungen – Ein Überblick über die verschiedenen Steuerarten, Wiesbaden (Springer Gabler), 2018.

Popov, Serguei: „The Tangle“, 2018, URL: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (abgerufen am 21. Okt. 2018).

PwC: „Blockchain und Smart Contracts“, 2017, URL: https://www.pwc.de/de/newsletter/it-security-news/blockchain-und-smart-contracts.html (abgerufen am 02. Nov. 2018).

PwC A: „Blockchain is here. What’s your next move?“, 2018, URL: https://www.pwc.com/blockchainsurvey (abgerufen am 03. Dez. 2018).

PwC B: „Blockchain in Financial Services – Mehr als nur ein Hype?“, 2018, URL: https://www.pwc.de/de/finanzdienstleistungen/Blockchain_in_Financial_Services_2018.pdf (abgerufen am 19. Nov. 2018).

Rauer, Nils; Bousonville, Ruth Maria: „Blockchain – tatsächliche und rechtliche Herausforderungen“, 2017, URL: http://hoganlovells-blog.de/2017/08/11/blockchain-tatsaechliche-und-rechtliche-herausforderungen/# (abgerufen am 01. Nov. 2018).

Rauschenberger, Pia: „Technologie schafft Transparenz: Blockchain in der Entwicklungszusammenarbeit“, 2017, URL: https://www.dw.com/de/technologie-schafft-transparenz-blockchain-in-der-entwicklungszusammenarbeit/a-40403614 (abgerufen am 01. Dez. 2018).

Richter, Bent: „Was ist IOTA?“, 2017, URL: https://www.kryptologen.de/2017/07/16/was-ist-iota/ (abgerufen am 21. Okt. 2018).

Rixecker, Kim: „Warum die Energiewirtschaft jetzt auf die Blockchain setzt“, 2017, URL: https://t3n.de/news/energiewirtschaft-blockchain-876165/ (abgerufen am 06. Dez. 2018).

Rogoff, Kenneth S.: Der Fluch des Geldes – Warum unser Bargeld verschwinden wird, München (FinanzBuch Verlag), 2016.

Roos, Alexander: „Private Keys: Wem gehören Deine Bitcoins?“, 2018, URL: https://www.btc-echo.de/private-keys-wem-gehoeren-deine-bitcoins/ (abgerufen am 22. Aug. 2018).

Rosenberger, Patrick: Bitcoin und Blockchain - Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin (Springer Vieweg), 2018.

Schäfer, Yvonne: „Smart Contracts – Intelligente Verträge der Zukunft?“, o. D., URL: https://www.skwschwarz.de/aktuelles/artikel/artikel-detail/news/smart-contracts-intelligente-vertraege-der-zukunft/4/detail/News/ (abgerufen am 05. Nov. 2018).

Schau, Tara: „Blockchain – Zukunftsmusik ohne rechtliche Realisierbarkeit?“, o. D., URL: http://rechtundnetz.com/blockchain-rechtliche-realisierbarkeit/ (abgerufen am 03. Nov. 2018).

Scheider, David: „IBM-Studie: Bitcoin, Krypto und die Zukunft des Geldes“, 2018, URL: https://www.btc-echo.de/ibm-studie-bitcoin-krypto-und-die-zukunft-des-geldes/ (abgerufen am 18. Nov. 2018).

Schickentanz, Chris-Oliver: „Fünf Jahre Nullzins enden: Experte erklärt, was jetzt das Beste für ihr Geld ist“, 2018, URL: https://www.focus.de/finanzen/experten/schickentanz/langsame-zinswende-erst-2021-hebt-die-ezb-den-zins-wieder-auf-inflationshoehe_id_9955301.html (abgerufen am 30. Nov. 2018).

Schmidt, Tobias A: „Visa und MasterCard: Kryptowährungen und ICOs als „hochriskant“ klassifiziert“, 2018, URL: https://www.btc-echo.de/visa-und-mastercard-kryptowaehrungen-und-icos-als-hochriskant-klassifiziert/ (abgerufen am 18. Nov. 2018).

Schmidt, Tobias B: „Volatilität: Krypto und Fiat im Vergleich“, 2018, URL: https://www.btc-echo.de/volatilitaet-krypto-und-fiat-im-vergleich/ (abgerufen am 24. Nov. 2018).

Schneider, Carmen: „Legal Update Energierecht: Blockchain in der Energiewirtschaft“, 2018, URL: https://w3.windmesse.de/windenergie/news/27569-blockchain-energiewirtschaft-energie-gesetz (abgerufen am 04. Dez. 2018).

Schrader, Christopher: „So teuer sind Bitcoin“, 2018, URL: https://www.sueddeutsche.de/digital/bitcoin-herstellung-energieverbrauch-1.4207289 (abgerufen am 21. Nov. 2018).

Schreder, Tim: Das neue Geld – Bitcoin, Kryptowährungen und Blockchain verständlich erklärt, München (Piper Verlag), 2018.

Schütte, Julian et al: „Blockchain und Smart Contracts – Technologien, Forschungsfragen, und Anwendungen“, 2017, URL: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf (abgerufen am 06. Dez. 2018).

Seitz, Johannes A: „Der Unterschied zwischen Coin und Token“, 2018, URL: https://thecoinscout.com/grundlagen/der-unterschied-zwischen-coin-und-token/ (abgerufen am 13. Okt. 2018).

Seitz, Johannes B: „Bitcoin-Hacking – Die Lücken des Rechts“, 2018, URL: https://www.lto.de/recht/hintergruende/h/bitcoin-wallet-schluessel-eigentum-besitz-hacker-rechtlicher-schutz/2/ (abgerufen am 04. Nov. 2018).

Siebert, Horst; Lorz, Oliver: Einführung in die Volkswirtschaftslehre, Stuttgart (Verlag W. Kohlhammer), 15. Auflage, 2007.

Sixt, Elfriede: Bitcoins und andere dezentrale Transaktionssysteme – Blockchains als Basis einer Kryptoökonomie, Wiesbaden (Springer Gabler), 2017.

Spancken, Marius et al.: „Kryptowährungen und Smart Contracts - Abschlussbericht zum Forschungs- und Entwicklungsprojekt 2015/2016“, 2016, URL: https://www.hb.fh-muenster.de/opus/fhms/volltexte/2016/1246/pdf/FuE_Kryptowaehrungen_und_Smart_Contracts_Abschlussbericht.pdf (abgerufen am 10. Nov. 2018).

Specht, Philip: Die 50 wichtigsten Themen der Digitalisierung – Künstliche Intelligenz, Blockchain, Bitcoin, Virtual Reality und vieles mehr verständlich erklärt, München (Redline Verlag), 2018.

Springer Professional: „Finanzbranche hat keine Eile mit der Blockchain“, 2018, URL: https://www.springerprofessional.de/bank-it/it-strategie/finanzbranche-hat-keine-eile-mit-der-blockchain-/15955814 (abgerufen am 19. Nov. 2018).

Stahl, Ernst et al.: E-Commerce-Leitfaden – Noch erfolgreicher im elektronischen Handel, Regensburg (Universitätsverlag Regensburg), 3. Auflage, 2012.

Statistisches Bundesamt: „Online-Banking in Deutschland beliebter als im EU-Durchschnitt“, 2017, Pressemitteilung Nr. 114, URL: https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2017/04/PD17_114_63931.html (abgerufen am 19. Jul. 2018).

Statistisches Bundesamt: „Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen)“, 2018, URL: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/ (abgerufen am 06. Aug. 2018).

Stein, Kathrin: „Blockchain – Basisinfos für Einsteiger“, 2017, URL: https://www.kryptologen.de/2017/08/18/blockchain-basisinfos-fuer-einsteiger/ (abgerufen am 25. Aug. 2018).

Stocker, Franz: „Bitcoin-Crash hat 600 Milliarden Dollar ausradiert“, 2018, URL: https://www.welt.de/finanzen/article181217212/Kryptowaehrungen-Bitcoin-Crash-hat-600-Milliarden-Dollar-ausradiert.html (abgerufen am 19. Aug. 2018).

Streim, Andreas; Britze, Nils: „Deutsche Wirtschaft zögert bei der Blockchain“, 2018, URL: https://www.bitkom.org/Presse/Presseinformation/Deutsche-Wirtschaft-zoegert-bei-der-Blockchain (abgerufen am 02. Dez. 2018).

Süme, Oliver; Vogt, Jan Niklas; Zimprich, Stephan: „Rechtliche Rahmenbedingungen der Blockchain“, in: „Blockchain – eine Technologie mit disruptivem Charakter“, 2018, S. 27 – 29, URL: https://www.vditz.de/fileadmin/media/bekanntmachungen/documents/vdi_publikation_blockchain_RZ_web_neu.pdf (abgerufen am 02. Nov. 2018).

Tagesspiegel: „Schürfen von Bitcoins verbraucht mehr Energie als ganz Dänemark“, 2018, URL: https://www.tagesspiegel.de/wirtschaft/herstellung-von-krypto-waehrung-schuerfen-von-bitcoins-verbraucht-mehr-energie-als-ganz-daenemark/23584446.html (abgerufen am 22. Nov. 2018).

Thiemann, Sophia: Blockchain: Blockchain und Bitcoins – Die Technologie der Zukunft, Berlin (Papyrus Autoren-Club), 2017.

Toggweiler, Patrick: „Krypto... WAS!?! Alles, was du über Bitcoin, Blockchain und Co. wissen musst“, 2017, URL: https://www.watson.ch/Wissen/Wirtschaft/694577558-Krypto----WAS----Alles--was-du-ueber-Bitcoin--Blockchain-und-Co--wissen-musst (abgerufen am 19. Jul. 2018).

Vennekel, Constantin: „Wie funktioniert Mining in Ethereum?“, 2018, URL: https://base58.de/wie-funktioniert-mining-in-ethereum/ (abgerufen am 10. Okt. 2018).

Wagenknecht, Sven: „Nasdaq verkündet positive Ergebnisse im Bereich Blockchain-Voting“, 2017, URL: https://www.btc-echo.de/nasdaq-verkuendet-positive-ergebnisse-im-bereich-blockchain-voting/ (abgerufen am 05. Dez. 2018).

Wenzel-Benner, Christian; Wasserrab, Daniel: „Kryptographische Hashfunktionen: Historie, Angriffe und aktuell sichere Standards“, o. D., URL: https://subs.emis.de/LNI/Proceedings/Proceedings240/79.pdf (abgerufen am 15. Sept. 2018).

Wiesner, Leonie: „Warum Charge Cards die beliebtesten Kreditkarten Deutschlands sind“, 2018, URL: https://www.focus.de/finanzen/banken/kreditkarten/charge-cards-das-sind-die-vorteile_id_8741066.html (abgerufen am 01. Aug. 2018).

Winheller A: „Initial Coin Offering (ICO)“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/ico-initial-coin-offering.html (abgerufen am 31. Okt. 2018).

Winheller B: „Die steuerliche Behandlung von Kryptowährungen in Deutschland“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/bitcoinundsteuer/besteuerung-kryprowaehrungen.html (abgerufen am 07. Nov. 2018).

Winheller C: „Bitcoin und Steuer“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/bitcoinundsteuer.html (abgerufen am 07. Nov. 2018).

Winheller D: „Besteuerung von Initial Coin Offerings (ICOs)“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/bitcoinundsteuer/besteuerung-ico.html (abgerufen am 07. Nov. 2018).

Winheller E: „Bitcoin, Regulierung und BaFin“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/bitcointrading/bitcoin-und-bafin.html (abgerufen am 10. Nov. 2018).

Winheller F: „Ethereum und Smart Contracts“, o. D., URL: https://www.winheller.com/bankrecht-finanzrecht/ethereum-smart-contracts.html (abgerufen am 05. Dez. 2018).

Wired: „Samsung will seine Lieferkette auf Blockchain umstellen“, 2018, URL: https://www.wired.de/collection/business/samsung-will-seine-lieferkette-auf-blockchain-umstellen (abgerufen am 02. Sept. 2018).

Witsch, Kathrin: „Blockchain-Technologie könnte die nächste Energiewende einleiten“, 2018, URL: https://www.handelsblatt.com/unternehmen/energie/strom-markt-blockchain-technologie-koennte-die-naechste-energiewende-einleiten/22837862.html?ticket=ST-1680943-rhTet07nKc7EAmgRMdxX-ap1 (abgerufen am 06. Dez. 2018).

Wozke, Martin: „3 Gründe, wieso Kryptowährungen volatil sind“, 2018, URL: https://blockchain-hero.com/3-gruende-wieso-kryptowaehrungen-volatil-sind/ (abgerufen am 24. Nov. 2018).

Xorbin: „SHA-256 hash calculator“, o. D., URL: https://www.xorbin.com/tools/sha256-hash-calculator (abgerufen am 11. Sept. 2018).

Zitzmann, Florian: „Steuerliche Behandlung der Kryptowährungen“, 2017, URL: https://www.haufe.de/compliance/management-praxis/steuerliche-behandlung-der-kryptowaehrungen_230130_431018.html (abgerufen am 06. Nov. 2018).

Zoller, Marcus: „Bitcoin und die Blockchain Technologie einfach erklärt“, 2017, URL: https://www.idnt.net/de-DE/blog/bitcoin-und-die-blockchain-technologie-einfach-erklaert (abgerufen am 22. Aug. 2018).

Eidesstattliche Versicherung

Ich versichere, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quelle kenntlich gemacht.

_____ _____

(Ort, Datum) (Unterschrift)

Einverständniserklärung

Ich erkläre mich damit einverstanden, dass ein Exemplar meiner Masterthesis in die Bibliothek des Fachbereichs aufgenommen wird; Rechte Dritter werden dadurch nicht verletzt.

_____ _____

(Ort, Datum) (Unterschrift)