BestMasters

Victor Rutz

Blockchain quo vadis

Eine Stärken-Schwächen-Analyse des Private- und des Public-Blockchain-Ansatzes

Springer Gabler

BestMasters

Mit **„BestMasters“** zeichnet Springer die besten Masterarbeiten aus, die an renommierten Hochschulen in Deutschland, Österreich und der Schweiz entstanden sind. Die mit Höchstnote ausgezeichneten Arbeiten wurden durch Gutachter zur Veröffentlichung empfohlen und behandeln aktuelle Themen aus unterschiedlichen Fachgebieten der Naturwissenschaften, Psychologie, Technik und Wirtschaftswissenschaften. Die Reihe wendet sich an Praktiker und Wissenschaftler gleichermaßen und soll insbesondere auch Nachwuchswissenschaftlern Orientierung geben.

Springer awards **“BestMasters”** to the best master’s theses which have been completed at renowned Universities in Germany, Austria, and Switzerland. The studies received highest marks and were recommended for publication by supervisors. They address current issues from various fields of research in natural sciences, psychology, technology, and economics. The series addresses practitioners as well as scientists and, in particular, offers guidance for early stage researchers.

Weitere Bände in der Reihe http://www.springer.com/series/13198

Victor Rutz

Blockchain quo vadis

Eine Stärken-Schwächen-Analyse des Private- und des Public-Blockchain-Ansatzes

Springer Gabler

Victor Rutz
Chemnitz, Deutschland

ISSN 2625-3577 ISSN 2625-3615 (electronic)
BestMasters
ISBN 978-3-658-29404-5 ISBN 978-3-658-29405-2 (eBook)
https://doi.org/10.1007/978-3-658-29405-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort

Seit einigen Jahren werden Geschäftsprozesse zunehmend durch Blockchains abgebildet und dokumentiert. Anwendungsgebiete sind Verträge aller Art, nicht nur von Banken und Versicherungen, sondern auch von IT- und Industrieunternehmen. Zwischen privat und öffentlich abgelegten Blockchains gibt es jedoch bedeutende Unterschiede, etwa hinsichtlich Verarbeitungsgeschwindigkeit oder Speicherplatzbedarf. Die Arbeit von Herrn Rutz enthält eine systematische Analyse der Stärken und Schwächen beider Blockchainvarianten.

Herr Rutz führt zunächst sehr differenziert in die Distributed-Ledger-Technologie, Kryptowährungen und Blockchains ein und erläutert die angewendeten Verschlüsselungsmethoden. Private und öffentliche Blockchains werden dann anhand der Kriterien Datenschutz, Sicherheit der Intermediäre, Konsensmechanismus, Redundanz, Leistungsfähigkeit, Settlement, Manipulationsresistenz sowie Energieeffizienz verglichen. Die inhaltliche Schwerpunktsetzung ist ausgewogen, und durch die detaillierte Betrachtung der Stärken und Schwächen beider Ansätze gibt Herr Rutz den aktuellen Stand der Literatur sehr gut wieder.

Thomas Maurer

Vorwort

In diesem Vorwort möchte ich mich bei all denjenigen bedanken, die mich während meines Bildungsweges begleitet haben und durch ihre fachliche oder ihre persönliche Unterstützung zum Gelingen dieser Masterarbeit beigetragen haben. Auch Springer Gabler möchte ich für die Auswahl meiner Arbeit für die Buchreihe „BestMasters“ danken. Diese Auszeichnung ehrt mich sehr.

Die vorliegende Arbeit entstand als Abschlussarbeit im Rahmen meines Masterstudiums an der Technischen Universität Chemnitz am Lehrstuhl für Finanzwirtschaft und Bankbetriebslehre von Prof. Dr. Thießen mit der persönlichen Betreuung durch Herrn Dr. Thomas Maurer. Herrn Dr. Maurer gilt für die anregenden Diskussionen und die wertvollen fachlichen Ratschläge mein größter Dank.

Neben der hervorragenden fachlichen Betreuung durch den Lehrstuhl für Finanzwirtschaft und Bankbetriebslehre habe ich während des gesamten Studiums im privaten Umfeld starken Rückhalt und Unterstützung erhalten, wofür ich meiner Familie von ganzem Herzen danken möchte. Hierbei möchte ich mich insbesondere bei meinem Bruder Thomas sowie bei Elvira und Simon für das Korrekturlesen und die emotionale Unterstützung in den kritischen Phasen des Studiums bedanken. Auch meinem Kommilitonen und gutem Freund Fabian danke ich für seine Unterstützung und sein fachliches Feedback. Mein besonderer Dank gilt meiner Freundin Helene, die mir stets den Rücken freigehalten hat und so maßgeblich dazu beigetragen hat, dass diese Masterarbeit in dieser Form vorliegt. Abschließend möchte ich von Herzen meiner Mutter Maria danken, deren Unterstützung mir mein Studium erst ermöglicht hat.

Victor Rutz

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ASIC	engl. Application-specific integrated circuit deut. anwendungsspezifische integrierte Stromkreise
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BFT	Byzantine Fault Tolerant
BOJ	Bank of Japan
BTC	Bitcoin
CPU	engl. Central processing unit deut. Zentralprozessor
DLT	Distributed Ledger Technologie
EBA	European Banking Authority
ETH	Ether
EZB	Europäische Zentralbank
GB	Gigabyte
GHOST	Greedy Heaviest Observed Subtree
GPU	engl. Graphics processing unit deut. Grafikprozessor
ILP	Interledger Protokoll
IP-Adresse	Internet-Protokoll-Adresse
ISO	International Organization for Standardization
METI	Ministry of Economy, Trade and Industry (Japan)
NONCE	Number Only Used Once
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerant
PoW	Proof-of-Work
RPCA	Ripple Protocol Consensus Algorithm

SWIFT	Society for Worldwide Interbank Financial Tele-communication
UNL	Unique Node List
UTXO	Unspent Transactions Output
VPN-Dienst	Virtual-Private-Network-Dienst
XRP	Ripple

1 Einführung

In diesem Kapitel erfolgt eine Einführung in die Thematik der vorliegenden Masterarbeit. Hierzu werden zunächst die Problemstellung sowie die Relevanz des Themas dargestellt. Anschließend werden die Zielsetzung und der Aufbau der Arbeit erläutert.

1.1 Problemstellung und Relevanz des Themas

„The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A. That kind of thing will develop on the Internet and that will make it even easier for people to use the internet."[1] Diese Aussage des renommierten Ökonomen FRIEDMAN aus dem Jahre 1999 wirkt im Kontext der aktuellen Diskussionen hinsichtlich des Potenzials einer neuen Technologie, welche vertrauenslose und anonyme Transaktionen zwischen unterschiedlichen Akteuren ermöglicht, geradezu prophetisch.[2] Besagte Technologie wird als Distributed Ledger Technology (DLT), oder aufgrund ihres einzigartigen Systems zur Archivierung von Transaktionen innerhalb einer linearen Kette aus kryptografisch verknüpften Blöcken auch als Blockchain, bezeichnet.[3] Bitcoin, der Prototyp dieser Technologie, wurde im Jahr 2008 in einem Arbeitspapier vorgestellt und ist ein Jahr später in Betrieb genommen worden.[4]

Während in den ersten Jahren nach Veröffentlichung des Prototyps seitens der Forschung kaum Interesse an der Technologie bestand,[5] wird sie heute als wichtigste technische Neuerung seit der Erfindung des Internets betrachtet.[6] Der Blockchain wird insbesondere in der Finanzwirtschaft ein höchst disruptives Potenzial zugeschrieben, welches zu einem regelrechten Paradigmenwechsel führen könnte.[7] Aber auch abseits der Finanzindustrie wird der Blockchain eine weitreichende Bedeutung unterstellt. Nach Einschätzung des World Economic Forums sollen beispielsweise im Jahr 2027 10% der globalen Wirtschaftsleistung auf der Blockchain gespeichert und verarbeitet werden.[8]

Den zahlreichen positiven Einschätzungen steht jedoch auch eine wachsende Anzahl an kritischen Meinungen gegenüber. In einer Befragung durch die Ibi Research-Gruppe der Universität Regensburg gaben 52% der befragten Experten im Bereich Digitalisierung an, dass das disruptive Potenzial der Blockchain überschätzt werde.[9] Andere Experten sehen die Blockchain und vor allem Bitcoin noch kritischer. Der US-Nationalökonom ROUBINI beispielsweise bezeichnet die Kursentwicklung Bitcoins gleichnamiger eigener Kryptowährung als *„Biggest Bubble in Human History"*[10] und vergleicht deren Preisentwicklung mit der Tulpenblase der 1630er Jahre.[11]

---

[1] Zitat: FRIEDMAN (1999).
[2] Vgl. SIXT (2017), S. 1.
[3] Vgl. BRÜHL (2017b), S. 135-137.
[4] Vgl. BOLESCH/MITSCHELE (2016), S. 35.
[5] Vgl. YLI-HUUMO ET AL. (2016), S. 9.
[6] Vgl. EFANOV/ROSCHIN (2018), S. 116.
[7] Vgl. BOLESCH/MITSCHELE (2016), S. 35.
[8] Vgl. World Economic Forum (2015), S. 24.
[9] Vgl. MESCH/JONIETZ/PETERS (2017), S. 7.
[10] Zitat: OSSINGER (2018).
[11] Vgl. OSSINGER (2018).

V. Rutz, *Blockchain quo vadis*, BestMasters,
https://doi.org/10.1007/978-3-658-29405-2_1

Neben den starken Kursschwankungen wird Bitcoin zunehmend auch hinsichtlich seiner hohen Transaktionskosten und des hohen Stromverbrauchs kritisiert. Nach Ansicht des Vorstandsmitgliedes der Bundesbank THIELE ist Bitcoin mittlerweile sowohl ökonomisch als auch ökologisch an seine Grenzen gestoßen.[12]

Bitcoin kann jedoch nicht als universeller Repräsentant für eine einheitliche Blockchain-Technologie angesehen werden. Stattdessen entwickelt eine Vielzahl an unterschiedlichen Akteuren verschiedene Blockchain-Lösungen mit unterschiedlichen Eigenschaften für unterschiedliche Anwendungsbereiche.[13] Bitcoin steht dabei als Archetyp für einen offenen und dezentralen Blockchain-Ansatz, dessen erklärtes Ziel die Schaffung eines Transaktionsnetzwerks ohne klassische Intermediäre wie z. B. Banken ist.[14] Dieser wird als **Public-Blockchain-Ansatz** bezeichnet.[15]

Gleichzeitig erkennen auch die traditionellen Intermediäre das Potenzial der DLT und nutzen einen anderen Implementierungsansatz dieser Technologie zur Schaffung und Umsetzung neuer Geschäftsmodelle.[16] Statt einem frei zugänglichen und dezentralen Aufbau konzentriert sich die Entwicklung dieses als **Private-Blockchain-Ansatz** bezeichneten Konzepts auf die Schaffung zugangsbeschränkter und zentralisierter Netzwerke.[17] Beide Ansätze haben sowohl Befürworter, als auch Kritiker und zeichnen sich durch individuelle Stärken und Schwächen aus.[18]

[12] Vgl. THIELE (2018).
[13] Vgl. MILKAU (2017), S. 24.
[14] Vgl. SWAN (2015), S. 85.
[15] Vgl. BaFin (2017).
[16] Vgl. SEITZ (2016), S. 166.
[17] Vgl. BaFin (2017).
[18] Vgl. BaFin (2017).

1.2 Zielsetzung und Aufbau der Arbeit

In der vorliegenden Masterarbeit soll die Distributed Ledger Technology bzw. die Blockchain kritisch beurteilt werden. Der Fokus liegt dabei auf einer differenzierten Betrachtung zuvor erwähnter Blockchain-Ansätze, wodurch festgestellt werden soll, ob einer der beiden Ansätze gegenüber dem anderen klare Vorteile aufweist und somit vorzuziehen ist. Dementsprechend kann folgende Forschungsfrage für die Untersuchung abgeleitet werden:

> *Ist einer der beiden Blockchain-Ansätze gegenüber dem anderen eindeutig vorzuziehen?*

Bei der Beschreibung der Problemstellung wurde zudem darauf hingewiesen, dass spezifische Blockchains in einigen Punkten bereits an die Grenzen der Leistungsmöglichkeiten gestoßen sein könnten. Hierdurch wären diese Blockchains für den weitreichenden Einsatz in bestimmten Bereichen, wie z. B. dem Massenzahlungsverkehr, ungeeignet.[19] Deshalb soll im Rahmen der Untersuchung neben einer Beurteilung von Stärken und Schwächen festgestellt werden, ob bestimmte Probleme gefunden werden, welche als unüberwindbare Hindernisse für eine weitreichende Implementierung angesehen werden können. Daher wird folgende zweite Forschungsfrage gestellt:

> *Existieren bestimmte Problemstellungen, die als unüberwindbare Hindernisse für eine weitreichende Implementierung eines der beiden, bzw. beider Blockchain-Ansätze angesehen werden können?*

Das Ziel der vorliegenden Masterarbeit ist die Beantwortung beider Forschungsfragen. Hierzu werden im weiteren Verlauf der Arbeit zunächst in Kapitel 2 die wesentlichen theoretischen Grundlagen beschrieben. Der Fokus liegt hierbei neben der Definition zentraler Begriffe in einer allgemeinen Darstellung der Blockchain, bzw. DLT. Im darauffolgenden Kapitel 3 werden anschließend die spezifischen Besonderheiten im Rahmen einer Stärken-Schwächen-Analyse verglichen. Abschließend werden im Kapitel 4 die Ergebnisse der Untersuchung zusammengefasst und kritisch gewürdigt, hierbei erfolgt auch die Beantwortung der beiden Forschungsfragen

[19] Vgl. THIELE (2018).

2 Theoretische Grundlagen

In diesem Kapitel erfolgt eine Darstellung der wesentlichen theoretischen Grundlagen. Es wird mit der Definition der Begriffe Intermediär, Blockchain, Distributed Ledger Technology und Kryptowährungen begonnen. Im Anschluss an die Beschreibung zentraler Begriffe werden, zum Verständnis der Funktionsweise einer Blockchain relevante, kryptografische Grundlagen erläutert. Im letzten Teil dieses Kapitels werden weitere Blockchain-Elemente beschrieben. Hierzu zählen die Wallet-Arten, die unterschiedlichen Arten von Netzwerkknoten und Möglichkeiten zur Lösung eines allgemeinen Problems verteilter Computersysteme, welches als das Problem byzantinischer Generäle bezeichnet wird.

2.1 Begriffserklärung und -abgrenzung

Die Begriffe Bitcoin, Blockchain und Distributed Ledger werden z. T. synonym zur Beschreibung unterschiedlicher Komponenten einer neuen Technologie verwendet. Hierzu nutzt beispielsweise SWAN den folgenden Vergleich: *„It is as if PayPal had called the Internet "PayPal" upon which the PayPal protocol was run, to transfer the PayPal currency."*[20] Für einen möglichst genauen Vergleich unterschiedlicher Blockchain-Ansätze ist allerdings eine trennscharfe Definition der verwendeten Begriffe notwendig. Deshalb werden im weiteren Verlauf dieses Abschnitts die Begriffe Kryptowährungen und Blockchain erklärt und von den aktuell genutzten Systemen, wie z. B. dem Zentralbankgeld und zentralisierten Datenbanken abgegrenzt. Vorher soll jedoch der Begriff Finanzintermediär definiert und dessen Aufgaben genauer betrachtet werden.

2.1.1 Finanzintermediäre

Für die Analyse der Blockchain-Technologie ist zunächst ein Verständnis hinsichtlich der Aufgaben von Finanzintermediären notwendig, da diese je nach Blockchain-Ansatz entweder ersetzt,[21] oder als Schnittstellen zwischen dem Ökosystem der Blockchain und der realen Welt eingebunden werden sollen.[22] AULIBAUER/THIEßEN definieren einen Finanzintermediär als *„Dienstleister, der im weitesten Sinne Angebot und Nachfrage am Kapitalmarkt koordiniert."*[23] Diese Koordination wird durch zahlreiche Leistungen erbracht, welche sich in die beiden Kategorien Vermittlungsleistungen und Transformationsleistungen einteilen lassen.[24] Eine detaillierte Betrachtung der Transformationsleistungen ist im Hinblick auf die Zielstellung der vorliegenden Masterarbeit nicht zielführend. Da die Blockchain die Vermittlungsleistung des Intermediäres substituieren soll,[25] wird stattdessen diese Leistungskategorie genauer betrachtet.

---

[20] Zitat: SWAN (2015), S. ix.
[21] Vgl. SWAN (2015), S. 85.
[22] Vgl. SIXT (2017), S. 180.
[23] Zitat: AULIBAUER/THIEßEN (2012), S. 43.
[24] Vgl. AULIBAUER/THIEßEN (2012), S. 44.
[25] Vgl. NAKAMOTO (2008), S. 1.

V. Rutz, *Blockchain quo vadis*, BestMasters,
https://doi.org/10.1007/978-3-658-29405-2_2

Aktuell zeichnen sich Finanztransaktionen durch eine hohe Anzahl an Intermediären aus,[26] deren Vermittlungsleistung folgende drei Funktionen erfüllen.[27]

- **Validierungsfunktion:**
  Der Intermediär überprüft im Vorfeld einer Transaktion, ob beide Transaktionspartner, also Käufer und Verkäufer sowie der Transaktionsgegenstand tatsächlich existieren und ob die Transaktion den rechtlichen und organisatorischen Anforderungen genügt.[28]
- **Abwicklungsfunktion:**
  Der Intermediär wickelt die Transaktion zwischen den beteiligten Marktteilnehmern ab. Dies beinhaltet auch das Clearing und Settlement.[29] Vereinfacht beschrieben erfolgt dies in zwei Schritten. Zunächst werden innerhalb des Clearings Forderungen und Verbindlichkeiten zweier Parteien auf- und verrechnet.[30] Anschließend werden diese im Settlement erfüllt.[31]
- **Aufzeichnungsfunktion:**
  Der Intermediär ist für die Aufzeichnung und Archivierung sämtlicher transaktionsrelevanter Daten verantwortlich. Hierdurch kann er im Falle nachträglicher (Rechts)-Streitigkeiten Nachweise zu Transaktionsinhalten liefern.[32]

Einige Autoren führen an, dass die Blockchain den Großteil der o. g. Funktionen von Intermediären erfüllen kann.[33] Allerdings erfüllen Intermediäre eine weitere Funktion. Sie können zu einer Reduktion von **Transaktionskosten** beitragen.[34] Der Begriff Transaktionskosten beschreibt sämtliche, im Zusammenhang mit einer Transaktion stehenden, Kosten. Hierbei handelt es sich u. a. um die Kosten für die Anbahnung, Vereinbarung, Abwicklung, Kontrolle und nachträgliche Anpassung eines Vertrages.[35]

Durch einen hohen Grad an Standardisierung der erbrachten Leistung und die Nutzung von Verbundvorteilen können Finanzintermediäre diese Kosten reduzieren.[36] Befürworter der Blockchain führen diesbezüglich jedoch an, dass durch das Entfernen der Intermediäre aus dem Transaktionsprozess eine noch stärkere Reduktion der Transaktionskosten möglich sei.[37] Blockchains nutzen hierzu eine dezentrale Netzwerkstruktur und eine eigene Form von virtuellem Geld, sog. Kryptowährungen.[38] Diese beiden Elemente sollen in den beiden folgenden Abschnitten genauer beschrieben werden. Hierzu wird zunächst der Begriff Kryptowährung definiert und vom aktuell genutzten Zentralbankgeld abgegrenzt.

---

[26] Vgl. Bundesbank (2017a), S. 39.
[27] Vgl. Mainelli/Millne (2016), S. 16.
[28] Vgl. Mainelli/Millne (2016), S. 16.
[29] Vgl. Seifert (2002), S. 24.
[30] Vgl. Metzger/Heldt/Hölscher (2018).
[31] Vgl. Heldt/Metzger (2018).
[32] Vgl. Mainelli/Millne (2016), S. 16.
[33] Vgl. Mainelli/Millne (2016), S. 17; vgl. Deubel/Moorman/Holotiuk (2017), S. 834.
[34] Vgl. Aulibauer/Thießen (2012), S. 53.
[35] Vgl. Aulibauer/Thießen (2012), S. 52 f.
[36] Vgl. Seifert (2002), S. 24 f.
[37] Vgl. Swan (2015), S. 85.
[38] Vgl. Swan (2015), S. ix f.

2.1.2 Kryptowährungen und virtuelles Geld

Laut THIELE sind aktuell ca. 1.400 unterschiedliche virtuelle Währungen, sog. Kryptowährungen, im Umlauf.[39] Obwohl es eine Vielzahl unterschiedlicher Blockchains mit einer eigenen Kryptowährungen gibt, sind diese keine zwingende Voraussetzung für den Aufbau und Betrieb einer Blockchain.[40] Kryptowährungen können in Blockchains dazu genutzt werden nahezu sofortige Zahlungen ohne den Einsatz von Intermediären durchzuführen.[41] Zudem dienen sie als Anreiz- und Entlohnungssystem für spezielle Netzwerkteilnehmer, welche z. T. sehr aufwendige Berechnungen durchführen und so zur Sicherheit und Stabilität des Netzwerks beitragen.[42] Neben dem Einsatz als Zahlungsmedium können Kryptowährungen auch als Repräsentant für die Besitzrechte an anderen realen Vermögenswerten, wie z. B. Wertpapieren, dienen. Folglich kann statt des Begriffs Kryptowährung auch der Begriff kryptografische Wertmarke, oder **Kryptotoken** verwendet werden.[43]

Die derzeit wohl bekannteste Kryptowährung ist Bitcoin.[44] Sie wurde zusammen mit dem gleichnamigen dezentralen Transaktionssystem im Jahre 2008 von NAKAMOTO[45] als ideologischer Gegenentwurf zum gängigen Zahlungssystem vorgestellt.[46] Die Einstufung von Kryptowährungen als virtuelles Geld wird allerdings in der Fachliteratur kontrovers diskutiert.[47] Um diese Kontroverse und die Funktion von Kryptowährungen besser zu verstehen empfiehlt es sich den Begriff Geld genauer zu betrachten. Nach MISHKIN muss jede Form von Geld drei wesentliche Funktionen erfüllen.[48]

- **Tauschmittelfunktion:**
  Geld muss dazu genutzt werden können, dieses gegen Waren und Dienstleistungen umtauschen zu können, um Transaktionskosten zu reduzieren und so die Effizienz des Handels zu steigern.[49]
- **Wertaufbewahrungsfunktion:**
  Da nicht jedes Wirtschaftssubjekt sein gesamtes Einkommen unmittelbar nach Erhalt wieder ausgeben möchte, muss Geld dazu genutzt werden können die erhaltene Kaufkraft über einen gewissen Zeitraum hinweg aufzubewahren.[50]
- **Recheneinheitsfunktion:**
  Geld muss zudem als verlässliche Recheneinheit fungieren. Hierunter ist zu verstehen, dass es dazu genutzt werden kann den Wert von Gütern und Dienstleistungen in einer

[39] Vgl. THIELE (2018).
[40] Vgl. BURGWINKEL (2016), S. 36.
[41] Vgl. BRÜHL (2017c), S. 371.
[42] Vgl. BURGWINKEL (2016), S. 36.
[43] Vgl. SWAN (2015), S. 71.
[44] Vgl. BURGWINKEL (2016), S. 23 und TURBAN ET AL. (2018), S. 484.
[45] Das Bitcoin Arbeitspapier wurde unter dem Pseudonym SATOSHI NAKAMOTO veröffentlicht. Die wahre Identität des Schöpfers der Kryptowährung ist nicht bekannt und wird ausgiebig diskutiert. Der interessierte Leser findet bei NARAYANAN ET AL. (2016), S. XXIII-XXVI eine detaillierte Beschreibung der Hinweise auf die Identität von NAKAMOTO.
[46] Vgl. SEITZ (2016), S. 165 f.
[47] Vgl. ALI ET AL. (2014), S. 279-281; vgl. THIELE/DIEHL (2017), S. 4 f.
[48] Vgl. MISHKIN (2016), S. 96.
[49] Vgl. MISHKIN (2016), S. 96 f.
[50] Vgl. MISHKIN (2016), S. 98.

> messbaren Form wiederzugeben.[51] Laut MISHKIN ist diese Funktion neben der Tauschmittelfunktion essenziell zur Reduktion von Transaktionskosten, da hierdurch ein einheitlicher Preis für gleiche Güter gebildet werden kann und somit nicht verschiedene Preise miteinander verglichen werden müssen.[52]

Gemäß diesen Funktionen ist Geld jedoch nicht zwangsläufig an einen physischen Gegenstand gebunden. Tatsächlich ist der Großteil der Geldmenge im Euro-Währungsgebiet lediglich in Form von Buchgeld als Bilanzposition in Datenbanken von Geschäfts- und Zentralbanken vorhanden.[53] Offizielle Währungen wie der Euro stellen eine Forderung gegenüber der Zentral- oder Geschäftsbank dar, weshalb sie als Forderungsgeld bezeichnet werden können. Der Wert dieses Forderungsgeldes ist somit an zentrale Institutionen geknüpft und verändert sich dementsprechend mit dem Vertrauen in besagte Institution.[54]

NAKAMOTO sieht gerade diese Abhängigkeit vom Vertrauen in zentrale Institutionen als Schwäche des aktuellen Zahlungssystems und schlug deshalb ein Zahlungssystem vor, welches das Vertrauen in zentrale Institutionen und Intermediäre überflüssig macht. Dies soll dadurch erreicht werden, dass das Vertrauen in zentrale Institutionen durch das Vertrauen in die verwendeten kryptografischen Verfahren zur fälschungssicheren Übermittlung von virtuellem Geld in einem Peer-to-Peer (P2P)-Netzwerk ersetzt wird.[55] Die Idee für digitales Geld ist bereits mehr als 30 Jahre vor der Einführung des Bitcoin diskutiert worden.[56] Die naheliegende Idee Geld ähnlich wie E-Mails von Wirtschaftssubjekt an Wirtschaftssubjekt über das Internet zu versenden stößt allerdings auf ein zentrales Problem, die sog. **Double Spending-Problematik**, welches sich in zwei Teilprobleme unterteilen lässt. Zum einen bestünde bei einem derartigen Transaktionssystem das Problem der **unendlichen Kopierbarkeit.** Versendet man eine virtuelle Geldnote per E-Mail, wird statt der eigentlichen Geldnote eine Kopie versendet.[57] Hierdurch könnte die virtuelle Geldnote wiederum **mehrfach ausgegeben** werden.[58]

Zur Lösung des Double Spending-Problems erhalten Kryptotokens einerseits eine individuelle Identifikationsnummer, ähnlich der Seriennummer auf Geldscheinen. Hierdurch ist jeder Kryptotoken einzigartig und identifizierbar.[59] Allerdings reicht ein Identifizierungsmerkmal alleine nicht zur Vermeidung des Double Spendings aus. Erst durch eine Dokumentation der Eigentumsübertragung kann eine mehrfache Ausgabe verhindert werden.[60] In zentralisierten Systemen erfassen vertrauenswürdige Intermediäre wie z. B. die Zentralbank Eigentumsübertragungen in einem Transaktionsbuch (engl. Ledger) und verhindern somit die mehrfache Ausgabe desselben Gegenstandes. Durch den Einsatz der Distributed Ledger Technology, bzw. der Blockchain ist dies allerdings auch ohne eine zentrale Instanz möglich.[61] Die Definition des

---

[51] Vgl. MISHKIN (2016), S. 97.
[52] Vgl. MISHKIN (2016), S. 97 f.
[53] Vgl. Bundesbank (2017b), S. 71.
[54] Vgl. THIELE (2017), S. 15.
[55] Vgl. NAKAMOTO (2008), S. 1.
[56] Vgl. EFANOV/ROSCHIN (2018), S. 116; vgl. MÖSER/BÖHME/BREUKER (2013), S. 10.
[57] Vgl. SWAN (2015), S. 2; vgl. MORABITO (2017), S. 6.
[58] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 35 f.
[59] Vgl. NARAYANAN ET AL. (2016), S. 21.
[60] Vgl. SWAN (2015), S. 2; vgl. MORABITO (2017), S. 6.
[61] Vgl. MORABITO (2017), S. 6.

Begriffs DLT zusammen mit einer Erklärung, wie diese Technologie das Double Spending Problem lösen kann, erfolgt im nächsten Abschnitt.

2.1.3 Distributed Ledger Technology und Blockchain

Distributed Ledger Technology lässt sich mit „Technologie verteilter Kontobücher" übersetzen.[62] Der Begriff beschreibt ein Verfahren bei dem das gemeinsam genutzte Transaktionsregister in einem **verteilten Netzwerk**, gespeichert und verarbeitet wird.[63] Im Gegensatz zu aktuell genutzten zentralisierten Datenbanken, bei denen das Kontobuch auf einem einzelnen Computer gespeichert wird, sind alle Netzwerkteilnehmer eines Distributed Ledgers miteinander verbunden und die Transaktionsdaten werden nicht nur dezentral gespeichert, sondern auf allen Geräten verteilt.[64] Dies ist in Abbildung 1 grafisch dargestellt.

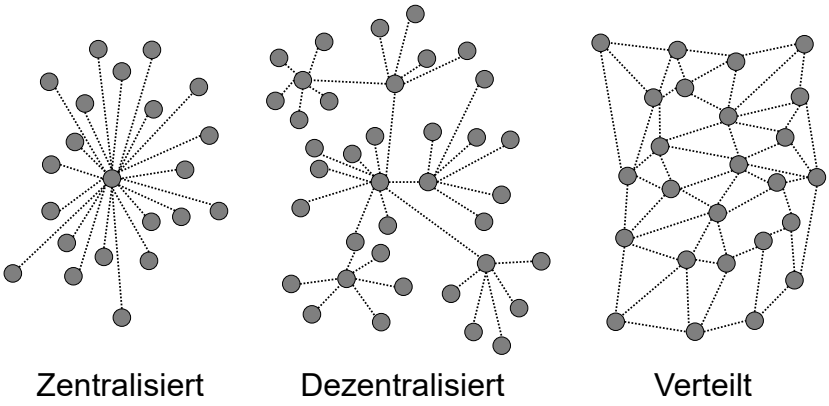


Abbildung 1: Aufbau zentraler, dezentraler und verteilter Systeme[65]

Neben der Verteilung der Datenbank unterscheiden sich DLT-Systeme auch durch ihre einzigartige Art der Dokumentation von Transaktionsdaten von ihrem zentralisierten Konterpart. In Distributed Ledgern werden Transaktionen zu Blöcken zusammengefasst, welche mithilfe kryptografischer Verfahren linear miteinander verknüpft werden und so die namensgebende Blockkette (engl. Blockchain) erzeugen.[66] An dieser Stelle ist anzumerken, dass zur Nutzung einer Blockchain nicht zwangsläufig ein P2P-Netzwerk verwendet werden muss. Es ist theoretisch auch möglich eine Blockchain auf einem einzigen lokalen Gerät, also ohne die gleichzeitige Nutzung eines verteilten Netzwerkes, zu implementieren.[67] Im weiteren Verlauf der vorliegenden Arbeit wird allerdings stets die Verwendung der Blockchain mit der komplementären

[62] Vgl. BURGWINKEL (2016), S. 9.
[63] Vgl. BRÜHL (2017b), S. 140.
[64] Vgl. GREENSPAN (2016), S. 175.
[65] Quelle: Adaptiert nach HOFMANN/STREWE/BOSIA (2018), S. 36; mit freundlicher Genehmigung von © Springer International Publishing AG.
[66] Vgl. BRÜHL (2017b), S. 137.
[67] Vgl. PLOOM (2016), S. 123.

Nutzung eines verteilten Netzwerks unterstellt, d. h. die Begriffe Blockchain und Distributed Ledger Technology werden nachfolgend synonym genutzt.

Das zentrale Element der Blockchain ist der Einsatz kryptografischer Verfahren zur Bestätigung und Durchführung von Transaktionen.[68] Mithilfe kryptografischer Verfahren werden gleich mehrere Probleme gelöst. Zum einen werden diese bei den sog. Konsensmechanismen zur Lösung des Koordinationsproblems zwischen den Netzwerkteilnehmern verteilter Netzwerke eingesetzt.[69] Gleichzeitig wird auch das Double Spendig durch den Einsatz kryptografischer Signaturen sowie durch die kryptografischen Verkettung der Transaktionsblöcke verhindert.[70] Aufgrund der hohen Bedeutung der Kryptografie für den effektiven Einsatz der Blockchain werden in den nächsten Abschnitten essentielle kryptografische Verfahren und deren Einsatz in der Blockchain erläutert.

2.2 Kryptografische Grundlagen

Der Begriff Kryptografie umfasst verschiedenste Verfahren zum Verstecken und Verschlüsseln von Informationen. Erste historische Belege für die Anwendung kryptografischer Verfahren werden auf ca. 2000 v. Chr. datiert.[71] Im Verlauf der Geschichte sind diese kontinuierlich weiterentwickelt worden. Die Verwendung geheimer Symbole, wie beispielsweise spezieller Hieroglyphen,[72] ist infolge des technologischen Fortschritts dabei sukzessiv durch z. T. sehr komplexe mathematische Verfahren ersetzt worden. Hierdurch ist die moderne Kryptografie als Teildisziplin der Mathematik anzusehen.[73] Im Kontext moderner Kommunikationstechniken lässt sich der Begriff Kryptografie dementsprechend folgendermaßen definieren: *„Kryptografie ist eine öffentliche mathematische Wissenschaft, in der Vertrauen geschaffen, übertragen und erhalten wird.“*[74] Die Verwendung mathematischer Verfahren bietet den Vorteil, dass moderne Kryptographieverfahren Vertrauen nicht durch die Geheimhaltung der Technologie schaffen, sondern durch die Tatsache, dass deren Qualität quantifizierbar und mathematisch beweisbar ist.[75] Zur kritischen Betrachtung von Stärken und Schwächen der Blockchain ist ein Verständnis der eingesetzten kryptografischen Verfahren notwendig. Hierzu werden im Nachfolgenden die Begriffe symmetrische und asymmetrische Verschlüsselung sowie Hash-Funktionen kurz erklärt. Nach der Beschreibung der Verfahren wird ihre Nutzung im Rahmen der Blockchain dargestellt.

2.2.1 Symmetrische und asymmetrische Verschlüsselung

Zur Verschlüsselung von Nachrichten können symmetrische und asymmetrische Verfahren genutzt werden. **Symmetrische Verfahren** zeichnen sich dadurch aus, dass bei der Kommunikation zwischen zwei Teilnehmern ein gemeinsamer Schlüssel zur Ver- und Entschlüsselung von

---

[68] Vgl. SEITZ (2016), S.168; vgl. ESMA (2016), S. 8.
[69] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 40.
[70] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 37.
[71] Vgl. PAAR/PELZL (2016), S. 1 f.
[72] Vgl. PAAR/PELZL (2016), S. 1.
[73] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 1.
[74] Zitat: BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S.1.
[75] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 1.

Nachrichten verwendet wird.[76] Bei diesen Verfahren besteht jedoch das Problem, dass der Schlüssel auf einem sicheren Weg übertragen werden muss, da im Falle eines kompromittierten privaten Schlüssels die Vertraulichkeit der Nachricht zerstört würde.[77] Das Problem kann allerdings durch die Nutzung eines asymmetrischen Verfahrens gelöst werden. Im Gegensatz zu symmetrischen Verschlüsselungsverfahren verwenden sämtliche Teilnehmer bei den **asymmetrischen Verfahren**, sog. **Public Key-Verfahren**, ein kryptografisch verknüpftes Schlüsselpaar. Dieses besteht aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key) zur Kodierung, bzw. Dekodierung der Nachrichten. Der öffentliche Schlüssel ist, wie der Name impliziert, öffentlich zugänglich und kann von allen Teilnehmern genutzt werden, um Nachrichten zu verschlüsseln. Der private Schlüssel hingegen ist nur dem Empfänger der Nachricht bekannt und dient zur Entschlüsselung der zuvor mithilfe des dazugehörigen öffentlichen Schlüssels kodierten Nachricht.[78]

PAAR/PELZL vergleichen die Systematik der Public Key Verschlüsselung mit der eines Briefkastens. In diesem Beispiel erfüllt der öffentliche Schlüssel dieselbe Funktion wie ein öffentlich zugänglicher Briefkasten, da jeder vorbeigehende Passant einen Brief in den Kasten einwerfen kann. Der Inhalt des Briefkastens kann jedoch nur von einer Person mit dem passenden Schlüssel, dem Private Key, eingesehen werden.[79] Dementsprechend muss bei der Erzeugung der Schlüsselpaare beachtet werden, dass die Möglichkeit zur Ableitung des privaten Schlüssels durch Analyse des öffentlichen Pendants ausgeschlossen ist.[80] Die Funktion der Public Key Verschlüsselung innerhalb einer Blockchain soll im Nachfolgenden anhand einer Bitcoin Transaktion verdeutlicht werden. In diesem Beispiel möchte eine Person einen Bitcoin an eine andere Person übertragen. Die Systematik wird in der Abbildung 2 zunächst grafisch dargestellt und anschließend erläutert.

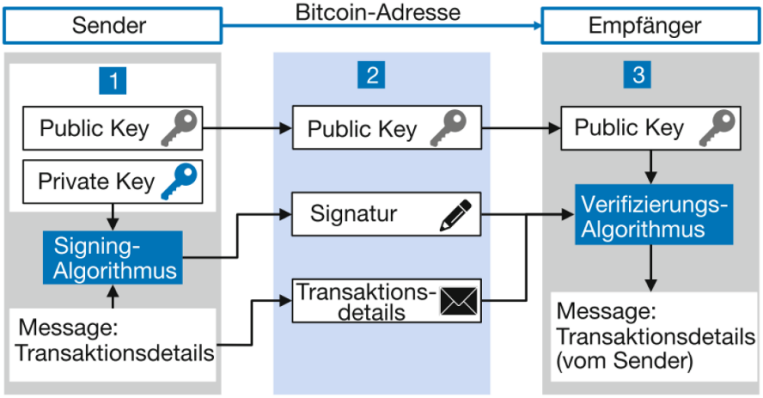


Abbildung 2: Nutzung des Public Key Verfahrens im Rahmen einer Bitcoin Transaktion[81]

[76] Vgl. SEITZ (2016), S. 168; vgl. PAAR/PELZL (2016), S. 174 f.
[77] Vgl. PETRLIC/SORGE (2017), S. 15.
[78] Vgl. PAAR/PELZL (2016), S. 176; vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 6.
[79] Vgl. PAAR/PELZL (2016), S. 176.
[80] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 106 f; vgl. BOLESCH/MITSCHELE (2016), S. 36.
[81] Quelle: Aus BRÜHL (2017b), S. 136; mit freundlicher Genehmigung von © ZBW und Springer-Verlag Berlin Heidelberg.

In Blockchains werden Akteure nicht über ihre persönlichen Daten identifiziert, stattdessen fungiert eine Einwegfunktion, ein sog. Hash[82] des öffentlichen Schlüssels, als Identität der Akteure und Zieladresse für Transaktionen.[83] Um Transaktionen zu tätigen benötigen beide Transaktionspartner folglich ein eigenes Schlüsselpaar, bestehend aus öffentlichem und privatem Schlüssel.[84] Zu Beginn einer Transaktion werden deren Details, also Höhe des Zahlungsbetrages und die Transaktionshistorie des übermittelten Bitcoins, welche den Sender als rechtmäßigen Eigentümer des Bitcoins ausweist, sowie die Bitcoin-Adresse des Empfängers mithilfe des Private Keys signiert. Anschließend werden diese Informationen zusammen mit dem Public Key des Senders an den Empfänger übermittelt.[85] Nach Erhalt der Nachricht kann der Empfänger den Public Key des Senders zur Verifizierung der Transaktion nutzen.[86] Da die Signierung der Transaktionsdetails ausschließlich mithilfe des dazugehörigen Private Keys möglich ist, kann der Empfänger zuverlässig feststellen, ob der Sender zum Zeitpunkt der Übertragung tatsächlich im Besitz des gesendeten Bitcoins war. Hierdurch kann verhindert werden, dass ein Netzwerkteilnehmer Transaktionen tätigt, obwohl er nicht über die benötigte Menge an Kryptotokens verfügt.[87]

Die Verwendung asymmetrischer Verschlüsselungsverfahren alleine verhindert jedoch nicht, dass einzelne Teilnehmer die betreffenden Tokens bereits vorher schon für Zahlungen verwendet haben.[88] Da in dezentralen Netzwerken die einzelnen Teilnehmer innerhalb eines P2P-Netzwerks gemeinsam für die Bestätigung von Transaktionen und deren Aufzeichnung verantwortlich sind, kann es infolge von Verzögerungen bei der Übertragung zu unerwünschtem Verhalten, wie z. B. der mehrfachen Ausgabe von Kryptotokens oder anderen Unstimmigkeiten bezüglich der Transaktionshistorie kommen.[89] Um dem entgegenzuwirken werden Transaktionen an alle Netzwerkteilnehmer gesendet und anschließend zu Blöcken zusammengefasst, welche mithilfe von Hash-Funktionen kryptografisch miteinander verknüpft werden.[90] Deren Funktionsweise wird im nächsten Abschnitt genauer beschrieben.

[82] Hash-Funktionen werden im nachfolgenden Abschnitt 2.2.2 genauer besprochen.
[83] Vgl. GEILING (2016), S. 28 f; vgl. STOMMEL (2017), S. 10; vgl. GREENSPAN (2016), S. 174.
[84] Vgl. BRÜHL (2017b), S. 136.
[85] Vgl. BRÜHL (2017b), S. 136.
[86] Vgl. BRÜHL (2017c), S. 371; vgl. PETRLIC/SORGE (2017), S. 82.
[87] Vgl. BRÜHL (2017b), S. 136; vgl. GEILING (2016), S. 29.
[88] Vgl. GEILING (2016), S. 29.
[89] Vgl. PINNA/RUTTENBERG (2016), S. 8.
[90] Vgl. BRÜHL (2017b), S. 136 f; vgl. PETRLIC/SORGE (2017), S. 82 f.

2.2.2 Hash-Funktionen

Bei Hash-Funktionen handelt es sich um sog. **Kompressionsfunktionen.** Dies bedeutet, dass Hash-Funktionen Nachrichten mit beliebiger Zeichenlänge in eine Bitfolge mit fester Zeichenlänge umrechnen.[91] Zur Veranschaulichung dieser Funktion, dient die Tabelle 1, welche die Hash-Werte zu unterschiedlichen Teilen des Titels der vorliegenden Arbeit zeigt.

Eingabetext (Input)	**Hash-Wert** (Output)
Blockchain quo vadis?	ac953b05d3c25321a025fa1ab82e582 442f5f765124ebdfa28f82691d7652a4c
Blockchain quo vadis? – Eine Stärken-Schwächen-Analyse des Private- und des Public-Blockchain-Ansatzes.	2b04989684eea5d8f4ffaecf84063e61 de48ea6be904fcab55c0b1576712a853

Tabelle 1: Hash-Länge bei unterschiedlich langem Inputtext[92]

Die Hash-Werte wurden mithilfe des Secure Hash Algorithmus (SHA)-256 erzeugt, welcher für einen beliebigen Eingabetext (Input) einen hexadezimalen Hash-Wert mit einer Länge von 64 Zeichen erzeugt.[93] Wie in der Tabelle 1 zu sehen ist, erzeugen sowohl ein Teilstück, als auch der vollständige Titel der vorliegenden Arbeit einen Hash-Wert mit der gleichen Anzahl an Zeichen.

Neben der Kompressionseigenschaft müssen Hash-Funktionen noch zwei weitere Eigenschaften erfüllen. Zum einen müssen sie **Einwegfunktionen** darstellen. Hierunter ist zu verstehen, dass zwar zu jeder Nachricht ein passender Hash-Wert erzeugt werden kann, ein umgekehrtes Vorgehen darf jedoch nicht möglich sein. Zum anderen müssen sie **kollisionsresistent** sein. Bei einer Kollision handelt es sich in diesem Kontext um den Fall, dass zwei verschiedene Nachrichten den gleichen Hash-Wert erzeugen.[94] Eine vollständige Vermeidung von Kollisionen ist nicht möglich, stattdessen müssen Hash-Funktionen stark kollisionsresistent sein. Hierunter ist zu verstehen, dass es zwar Kollisionen geben darf, ein effizientes Verfahren zu deren Ermittlung darf jedoch nicht möglich sein.[95] Hierdurch ist der Hash-Wert einer Nachricht beliebiger Länge nahezu einzigartig und als dessen kryptografischer Fingerabdruck anzusehen, bei dem bereits kleinste Änderungen des Inputs eine vollständige Veränderung des Hash-Wertes zur Folge haben.[96]

Diese Funktion soll ebenfalls anhand eines Beispiels gezeigt werden. Hierzu wurden in der Tabelle 2 für den jeweils eingegebenen Text mithilfe eines SHA-256-Rechners entsprechende Hash-Werte erzeugt. Als Eingabetext wurde in beiden Fällen der Haupttitel der vorliegenden Masterarbeit gewählt, jedoch wurde im unteren Eingabetext das Fragezeichen durch ein Ausrufezeichen ersetzt. Wie in Tabelle 2 zu sehen ist, hat bereits eine geringfügige Veränderung der Input-Variablen eine vollständige Veränderung des erzeugten Outputs zur Folge.

---

[91] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 176; vgl. PAAR/PELZL (2016), S. 335.
[92] Quelle: Eigene Darstellung, basierend auf den Ergebnissen des Hash-Rechners von Xorbin (2018).
[93] Vgl. BRÜHL (2017c), S. 372.
[94] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 110.
[95] Vgl. BEUTELSPACHER/NEUMANN/SCHWARZPAUL (2010), S. 177.
[96] Vgl. PAAR/PELZL (2016), S. 335.

Eingabetext (Input)	**Hash-Wert** (Output)
Blockchain quo vadis?	ac953b05d3c25321a025fa1ab82e5824 42f5f765124ebdfa28f82691d7652a4c
Blockchain quo vadis!	bd28bdd7eab235739c017ea0b96d2e6c 694b00ccab42c0ee88a1999faf3ec290

Tabelle 2: Reaktion des Hash-Wertes auf Veränderung der Input-Variablen[97]

Die Verwendung von Hash-Funktionen ist neben dem Einsatz des Public-Key-Verfahrens ein zentrales Element in der Blockchain, da die Verkettung der einzelnen Blöcke mithilfe von Hash-Funktionen erreicht wird.[98] Dabei hat jeder Block innerhalb der Kette einen ähnlichen Aufbau. Dieser kann vereinfacht in die zwei Bereiche **Header** und **Transaktionen** unterteilt werden.[99] Im Transaktionsteil werden noch nicht bestätigte Transaktionen gesammelt und anschließend zu Paaren zusammengefasst, wobei aus den Hash-Werten jedes Paares ein gemeinsamer Hash-Wert erzeugt wird. Dieser Vorgang wird danach sukzessiv für alle neu ermittelten Hash-Werte durchgeführt, bis kein weiterer Hash für eine Paarbildung verbleibt.[100] Dieser Vorgang ist in der nachfolgenden Abbildung 3 grafisch dargestellt.

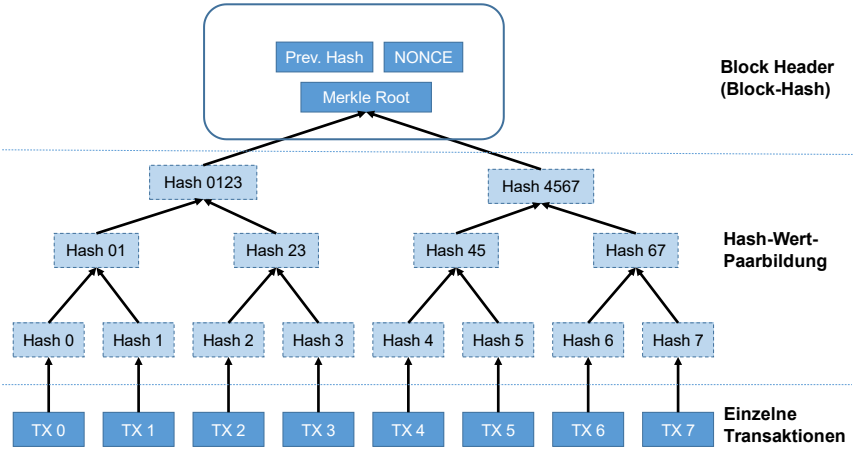


Abbildung 3: Darstellung eines Merkle Trees innerhalb eines Transaktionsblocks[101]

[97] Quelle: Eigene Darstellung, basierend auf den Ergebnissen des Hash-Rechners von Xorbin (2018).
[98] Vgl. METI (2016), S. 11.
[99] Vgl. PARK/PARK (2017), S. 2.
[100] Vgl. BRÜHL (2017b), S. 137.
[101] Quelle: Eigene Darstellung, in Anlehnung an NAKAMOTO (2008), S. 4.

Dieses Verfahren geht auf MERKLE zurück und wird aufgrund der Ähnlichkeit mit der Aststruktur eines Baumes als **Merkle Tree** bezeichnet.[102] Der letzte Hash stellt dabei die „Wurzel" des Baumes dar und wird dementsprechend **Merkle Root** genannt.[103] Die Merkle Root wird zusammen mit dem finalen Hash-Wert des vorangegangen Transaktionsblocks in den Header des aktuellen Blocks aufgenommen. Anschließend wird ein einzigartiger blockspezifischer Wert, die sog. **Number Only Used Once (NONCE)** ermittelt. Schließlich wird aus den Werten der Merkle Root, des finalen Hash-Wertes des vorangegangenen Blocks und der NONCE der finale Hash-Wert des aktuellen Blocks, der sog. **Block-Hash** erzeugt. Dieser dient wiederum als Referenzwert für den folgenden Block.[104] Diese Systematik wird in der Abbildung 4 grafisch dargestellt.

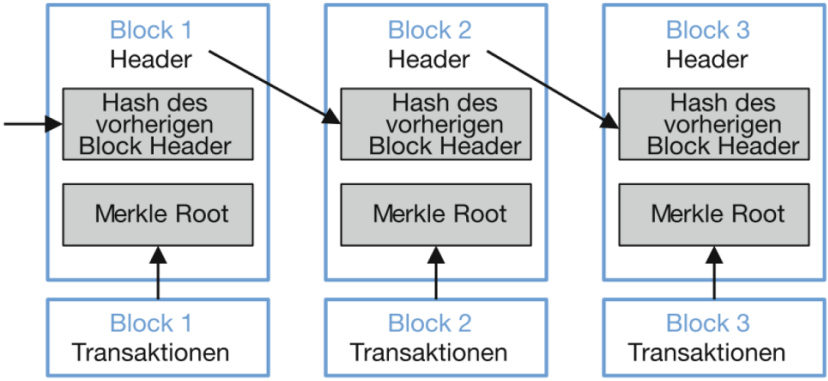


Abbildung 4: Verkettung der Blöcke mithilfe von Hash-Funktionen[105]

Das mehrfache „Hashen" der Transaktionsdetails führt dazu, dass selbst kleinste nachträgliche Änderungen sofort erkannt werden können.[106] Durch die Verkettung der einzelnen Blöcke müssten zudem zu einer nachträglichen Manipulation eines bestimmten Eintrages innerhalb der Blockchain auch für alle nachfolgenden Blöcke neue Hash-Werte ermittelt werden.[107] Um die Wahrscheinlichkeit für eine nachträgliche Manipulation zusätzlich zu reduzieren, wird zudem kein einfacher Hash-Wert erzeugt. Stattdessen ist der Aufbau des Block-Hashes an einen bestimmten Faktor gebunden. Hierbei handelt es sich um den Schwierigkeitsgrad. Dieser legt fest, dass der Block-Hash mit einer bestimmten Anzahl an Nullen beginnen muss.[108]

Da es bei stark kollisionsresistenten Hash-Verfahren, wie dem in den vorherigen Beispielen verwendeten SHA-256, kein effizientes Verfahren zur Ermittlung eines spezifischen Wertes geben darf,[109] müssen zur Ermittlung eines gültigen Hash-Wertes nacheinander zufällige

[102] Vgl. NARAYANAN ET AL. (2016), S. 12.
[103] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 40.
[104] Vgl. BRÜHL (2017b), S. 137.
[105] Quelle: Aus BRÜHL (2017b), S. 137; mit freundlicher Genehmigung von © ZBW und Springer-Verlag Berlin Heidelberg.
[106] Vgl. NARAYANAN ET AL. (2016), S. 13.
[107] Vgl. PETRLIC/SORGE (2017), S. 83; vgl. BRÜHL (2017b), S. 137.
[108] Vgl. PETRLIC/SORGE (2017), S. 83.
[109] Vgl. Abschnitt 2.2.2.

NONCE-Werte und Block-Hashes durchprobiert werden, bis ein geeigneter Wert gefunden wird.[110] Die Auswirkungen dieses, als **Mining** bezeichneten, Prozesses werden im Rahmen der Stärken-Schwächen-Analyse genauer betrachtet. Im weiteren Verlauf dieses Kapitels werden stattdessen weitere Elemente der Distributed Ledger Technology beschrieben.

2.3 Weitere Elemente der Distributed Ledger Technology

Neben den kryptografischen Verfahren und dem verteilten Netzwerkaufbau weisen Blockchains weitere Elemente auf, deren individuelle Eigenschaften zur Beurteilung eines Blockchain-Ansatzes essenziell sind. Diese sollen im Nachfolgenden überblicksartig beschrieben werden. Dabei wird mit den Wallets begonnen. Hierbei handelt es sich um Softwareanwendungen, welche die Interaktion eines Wirtschaftssubjektes mit der Blockchain ermöglichen.[111] Danach werden die Rollen der Netzwerkteilnehmer beschrieben. Abschließend erfolgt eine kurze Darstellung des Koordinationsproblems verteilter Systeme, welches als Problem byzantinischer Generäle bezeichnet wird, sowie Möglichkeiten zu dessen Lösung.

2.3.1 Wallets

Der Begriff Wallet kann auf Deutsch mit Geldbörse übersetzt werden und stellt eine präzise Beschreibung der Hauptfunktion dieser Softwareanwendung dar, die Verwaltung von Kryptotokens. Mittlerweile existieren zahlreiche Wallet-Lösungen, welche jedoch allesamt folgende sechs Funktionen erfüllen.[112]

1. Möglichkeit zum Senden von Tokens
2. Möglichkeit zum Empfangen von Tokens
3. Sicherung des privaten Schlüssels
4. Möglichkeit zur Signierung von Nachrichten
5. Aufbewahrung und Verwaltung privater Schlüssel
6. Speicherung der eigenen Adressen in einem Adressbuch

Eine grobe Unterteilung der Wallets kann hinsichtlich On- und Offline Wallets getroffen werden. Bei Offline Wallets werden sämtliche relevante Daten lokal auf einem Rechner, einem USB-Stick oder auf einem speziell angefertigten Gerät, einer sog. Hardware Wallet, gespeichert.[113] Zudem kann ein sog. Cold Wallet genutzt werden, bei dem der private Schlüssel auf einem Blatt Papier ausgedruckt wird.[114]

Da die Transaktionshistorie im gesamten P2P-Netzwerk verteilt wird, entstehen in Blockchains Bedenken hinsichtlich des Schutzes der Privatsphäre. Um die Anonymität des Nutzers zu wahren wird bereits im Bitcoin-Arbeitspapier empfohlen für neue Transaktionen auch neue Adressen, also öffentliche Schlüssel, zu verwenden.[115] Da mit der Erzeugung eines neuen öffentlichen Schlüssels auch stets ein neuer privater Schlüssel generiert wird,[116] müsste bei ausschließlicher

---

[110] Vgl. BOLESCH/MITSCHELE (2016), S. 37.
[111] Vgl. BRÜHL (2017b), S. 136.
[112] Vgl. SIXT (2017), S. 36 f.
[113] Vgl. PLOOM (2016), S. 138.
[114] Vgl. STOMMEL (2017), S. 11; vgl. PLOOM (2016), S. 138.
[115] Vgl. NAKAMOTO (2008), S. 6.
[116] Vgl. Abschnitt 2.2.1.

Nutzung eines Cold Wallets stets ein neuer privater Schlüssel ausgedruckt werden. SIXT schlägt dementsprechend die kombinierte Nutzung von Online Wallets und Cold Wallets vor. Das Cold Wallet dient dabei als Rücklage für Kryptotokens, während das Online Wallet für den täglichen Gebrauch verwendet wird.[117] Dieses Vorgehen ist Vergleichbar mit der Nutzung von Sparbuch und Girokonto, wobei das Cold Wallet mit dem Sparbuch und das Online Wallet mit dem Girokonto verglichen werden kann. Viele Nutzer verzichten jedoch auf Offlinelösungen und nutzen ausschließlich ein Online, bzw. Web Wallet. Hierbei handelt es sich um Cloud Dienste, welche über ein Webinterface aufrufbar sind und somit orts-, bzw. geräteunabhänige Transaktionen ermöglichen.[118]

2.3.2 Full-Nodes und Thin-Nodes

Die Teilnehmer eines Netzwerks werden als Knoten (engl. Nodes) bezeichnet, diese können hinsichtlich ihres Leistungsbeitrags zum Netzwerk in Full-Nodes und Thin-Nodes eingeteilt werden. **Thin-Nodes** speichern im Gegensatz zur Full-Variante lediglich Header der Transaktionsblöcke sowie die eigenen Transaktionsdaten auf dem Gerät und nehmen demenentsprechend nicht am Bestätigungsprozess von Transaktionen teil.[119] In manchen Literaturquellen werden Thin-Nodes auch als Clients bezeichnet.[120]

Bei **Full-Nodes** hingegen handelt es sich um vollständige Knoten, welche jederzeit die vollständige Transaktionshistorie, also die gesamte Blockchain, auf ihrem Gerät speichern.[121] Neben der Speicherung der Transaktionshistorie sind Full-Nodes auch für die Verarbeitung von Transaktionen innerhalb des Netzwerkes zuständig.[122] Dementsprechend führen sie alle im Abschnitt 2.2.2 beschriebenen Prozesse durch. Da alle Full-Nodes individuell an der Verarbeitung und Speicherung von Transaktionsdaten arbeiten, kann es zu Koordinationsproblemen zwischen den Full-Nodes kommen, welche diese durch einen Konsensmechanismus lösen.[123] Dies wird im nachfolgenden Abschnitt genauer erläutert.

2.3.3 Das Problem byzantinischer Generäle und Konsensmechanismen

Das Problem byzantinischer Generäle beschreibt eine Problemstellung verteilter Computersysteme, welche aufgrund von Verzögerungen bei der Datenübertragung, fehlerhafter Komponenten oder falscher Informationen von betrügerischen Netzwerkteilnehmer widersprüchliche Informationen erhalten. Trotz der unterschiedlichen Informationen müssen sämtliche Netzwerkknoten jedoch einen Konsens, also die Einigung auf bestimmtes Ergebnis erreichen.[124] Im Falle der Blockchain wäre dies die Einigung auf eine bestimmte Transaktionshistorie.[125]

Diese Problemstellung lässt sich am besten anhand der von LAMPORT/SHOSTAK/PAESE verwendeten Analogie hinsichtlich der Koordinationsprobleme einer Armee bei der Belagerung einer

---

[117] Vgl. SIXT (2017), S. 94.
[118] Vgl. SIXT (2017), S. 37.
[119] Vgl. SIXT (2017), S. 36.
[120] Vgl. VUKOLIĆ (2016), S. 117.
[121] Vgl. SIXT (2017), S. 35.
[122] Vgl. SIXT (2017), S. 39.
[123] Vgl. Bundesbank (2017a), S. 37.
[124] Vgl. LAMPORT/SHOSTAK/PEASE (1982), S. 382 f.
[125] Vgl. SÜRMELI ET AL. (2017), S. 597.

Stadt erklären. In diesem Beispiel besteht die Belagerungsarmee aus einzelnen Divisionen, welche um die Stadt herum verteilt sind und jeweils von einem General angeführt werden. Für einen erfolgreichen Angriff müssen sich die Generäle auf einen Plan einigen. Allerdings können sie untereinander nur mithilfe von Botschaftern kommunizieren. Diese Kommunikationsschwierigkeiten werden zudem dadurch erschwert, dass unter den Generälen auch Verräter sein könnten, welche absichtlich falsche Informationen versenden und hierdurch eine Einigung verhindern.[126] Dieses Problem wird in der Abbildung 5 dargestellt.

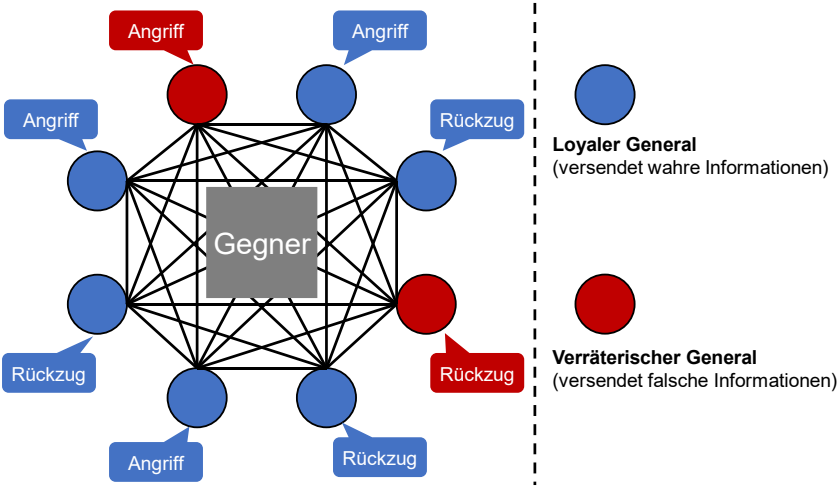


Abbildung 5: Das Problem byzantinischer Generäle[127]

Soll zur Lösung dieses Problems ein Algorithmus verwendet werden, muss dieser folgende zwei Bedingungen erfüllen. Zum einem müssen sich alle loyalen Generäle auf einen gemeinsamen Plan einigen. Zum anderen muss verhindert werden, dass eine kleine Anzahl an Verrätern die loyalen Generäle zur Durchführung eines schlechten Plans verleitet.[128] Im Kontext von Distributed Ledgern bedeutet dies, dass zwischen den Nodes ein **Konsens** erzielt werden muss, bei dem sich alle ehrlichen Netzwerkteilnehmer auf die korrekte Transaktionshistorie einigen können und sich nicht von betrügerischen Nodes zur Akzeptanz einer manipulierten Historie verleiten lassen.[129]

Das Konsensproblem wird von unterschiedlichen Blockchain-Varianten mit z. T. deutlich voneinander abweichenden Protokollen gelöst. Je nachdem, ob die Zielsetzung der Blockchain auf den Betrieb eines öffentlichen oder eines privaten Distributed Ledgers ausgerichtet ist, kommt es zu unterschiedlichen Konsenskonzepten.[130] Hierbei kann grob zwischen vertrauenslosen Konsensmechanismen, wie dem **Proof-of-Work (PoW)** und teilweise vertrauensbasierten

[126] Vgl. LAMPORT/SHOSTAK/PEASE (1982), S. 382 f.
[127] Quelle: Eigene Darstellung in Anlehnung an METI (2016), S. 12.
[128] Vgl. LAMPORT/SHOSTAK/PEASE (1982), S. 383.
[129] Vgl. LAMPORT/SHOSTAK/PEASE (1982), S. 383.
[130] Vgl. STOMMEL (2017), S. 8.

Konsensmechanismen, wie dem **Byzantine Fault Tolerant (BFT)** unterschieden werden.[131] Das PoW fordert von Netzwerkteilnehmern zur Bestätigung von Transaktionen einen Arbeitsnachweis in Form von Rechenleistung.[132] Beim BFT hingegen stimmen die beteiligten Full-Nodes über eine Änderung der Transaktionshistorie ab.[133] Transaktionsblöcke werden in diesem Konsensmodell bestätigt, wenn eine gewisse Mindestanzahl an Full-Nodes dem Hinzufügen eines Blockes zur Blockchain zustimmt.[134] Die Konsensmechanismen haben einen signifikanten Einfluss auf die zahlreiche Faktoren, wie z. B. die Leistungsfähigkeit oder Sicherheit einer Blockchain.[135] Dementsprechend werden sie innerhalb der Stärken-Schwächen-Analyse des nächsten Kapitels detailliert untersucht.

[131] Vgl. BALIGA (2017), S. 11.
[132] Vgl. Bundesbank (2017a), S. 38.
[133] Vgl. BALIGA (2017), S. 9 f.
[134] Vgl. Bundesbank (2017a), S. 38.
[135] Vgl. VUKOLIĆ (2016), S. 115.

3 Stärken-Schwächen-Analyse der Blockchain-Ansätze

In diesem Kapitel erfolgt die Beurteilung des Public- und des Private-Blockchain-Ansatzes im Rahmen einer Stärken-Schwächen-Analyse. Diese Untersuchung gliedert sich dabei in fünf aufeinanderfolgende Abschnitte. Im ersten Abschnitt erfolgt eine kurze Vorbetrachtung. Hierbei wird auf Basis unterschiedlicher Möglichkeiten zur Systematisierung von Blockchain-Typen eine Abgrenzung zwischen dem Private- und dem Public-Blockchain-Ansatz vorgenommen. Anschließend werden relevante Praxisbeispiele beider Ansätze in individuellen Kurzprofilen vorgestellt. Im zweiten Abschnitt erfolgt eine genaue Darstellung des Untersuchungsaufbaus. Neben einer Beschreibung der gewählten Untersuchungsmethode werden hierbei auch deren Spezifikationen wie z. B. die Zweiteilung der Analyse erläutert. Die darauffolgenden Abschnitte 3.3 und 3.4 stellen den Kern der Untersuchung dar. Hier sollen die jeweiligen Stärken und Schwächen der beiden Ansätze anhand eines Vergleichs unterschiedlicher Blockchain-typischer Elemente kritisch beurteilt werden. Abschließend werden im fünften und letzten Abschnitt die Ergebnisse der Untersuchung ausgewertet. Hierdurch sollen im nächsten Kapitel die beiden Forschungsfragen der vorliegenden Masterarbeit beantwortet werden.

3.1 Vorbetrachtung

Zu Beginn der Untersuchung erfolgt eine Darstellung von Möglichkeiten zur Systematisierung von Blockchain-Typen. Hierbei sollen die wesentlichen Unterschiede zwischen den beiden Blockchain-Ansätzen vorgestellt werden. Darauf folgend werden ausgewählte Praxisbeispiele vorgestellt, welche als Repräsentanten der beiden Ansätze im Rahmen der Analyse auf ihre Stärken und Schwächen hin untersuchten werden.

3.1.1 Systematisierung von Blockchain-Typen

Derzeit arbeiten zahlreiche FinTech-Startups, aber auch etablierte Unternehmen an der Entwicklung eigener Blockchainsysteme mit z. T. sehr unterschiedlicher Ausgestaltung und Einsatzmöglichkeiten.[136] Da diese Systeme ohne Kooperation mit Organisationen, wie z. B. der International Organization for Standardization (ISO) oder der International Swaps and Derivatives Association entstehen, sind sie größtenteils nicht an etablierte Normen und Standards angepasst.[137] Sie sind dementsprechend häufig nicht interoperabel und können daher nicht, oder nur bedingt zur gemeinsamen Lösung eines Problems verwendet werden.[138] Auch wenn übergreifende DLT-Standards bisher nicht vorhanden sind, lassen sich Blockchain-Ansätze dennoch in bestimmten Gruppen zusammenfassen bzw. voneinander abgrenzen. HILEMAN/RAUCHS z. B. ordnen Blockchains einer von vier Varianten zu, die sich hinsichtlich dreier Eigenschaften unterscheiden. Wie in Tabelle 3 zu sehen ist, werden bei dieser Typisierung Blockchains, in denen das Lesen der Transaktionsdaten ohne jegliche Einschränkung möglich ist, als

[136] Vgl. THIELE (2017), S. 14.
[137] Vgl. SWIFT (2016), S. 9.
[138] Vgl. SWIFT (2016), S. 9; vgl. HILEMAN/RAUCHS (2017), S. 74.

V. Rutz, *Blockchain quo vadis*, BestMasters,
https://doi.org/10.1007/978-3-658-29405-2_3

Public, bzw. open Blockchains klassifiziert. Demgegenüber stehen **Private**, bzw. closed Blockchains. Bei diesem Typus ist die Leseberechtigung auf eine bestimmte Menge an Teilnehmern oder Nodes beschränkt.[139]

			Read	Write	Commit	Example
Blockchain Types	Open	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

Tabelle 3: Ausgestaltungsmöglichkeiten der DLT nach HILEMAN/RAUCHS[140]

Sowohl private als auch öffentliche Blockchains können zusätzlich auch nach der Ausgestaltung der Zugriffs- und Mitbestimmungsrechte unterschieden werden. In diesem Fall unterscheidet man zwischen **erlaubnisfreien (permissionless)** und **erlaubnispflichtigen (permissioned)** Varianten.[141] Diese Attribute definieren den Grad der Mitwirkungsmöglichkeit innerhalb der Blockchain, also die Möglichkeit zur Durchführung von Transaktionen (write) sowie zur Veränderung des Aufbaus (commit). Während erlaubnisfreie Blockchains keinerlei Restriktionen in diesen Kategorien aufweisen, ist beim erlaubnispflichtigen Typus zur Ausübung der jeweiligen Aktionen eine vorherige Erlaubnis des Netzwerks oder einer zentralen Instanz notwendig. Zwischen den beiden Extremen Public Permissionless und Private Permissioned liegen jedoch auch **Hybridlösungen,** wie die Public Permissioned und Consortium Blockchains.[142]

Gemäß JUNG/PLAZIBAT ähneln Hybridlösungen zwischen dem Public- und dem Private-Blockchain-Ansatz, hinsichtlich der Leserechte eher der öffentlichen Variante. In Bezug auf die Mitwirkungsrechte ist dieser Typus jedoch ähnlich restriktiv wie die private Variante, da in beiden Fällen eine zentrale Partei notwendig ist, die den Zugang reguliert.[143] Aufgrund der restriktiven Natur und der Notwendigkeit einer zentralen Instanz werden Hybridlösungen im weiteren Verlauf der Untersuchung dem Private-Blockchain-Ansatz zugeordnet. Diese Zuordnung wird z. T. in der Forschung,[144] aber beispielsweise auch von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) getroffen. Laut BaFin können Blockchains in private, bzw. zentralisierte und

[139] Vgl. HILEMAN/RAUCHS (2017), S. 20.
[140] Quelle: Eigene Darstellung, in Anlehnung an HILEMAN/RAUCHS (2017), S. 20.
[141] Vgl. HILEMAN/RAUCHS (2017), S. 20.
[142] Vgl. HILEMAN/RAUCHS (2017), S. 20.
[143] Vgl. JUNG/PLAZIBAT (2017), S. 49.
[144] Vgl. VUKOLIĆ (2016), S. 115 f.

öffentliche, bzw. dezentralisierte Blockchains unterteilt werden. Der Typus „öffentlich“ umfasst dementsprechend alle Blockchains, die sämtlichen Nodes gleiche Rechte hinsichtlich der Einsicht in die Transaktionshistorie, die Initiierung von Transaktionen und deren Validierung zuweisen.[145] Private Blockchains sind hingegen nicht öffentlich zugänglich. Stattdessen wird der Zugang zur Blockchain durch eine zentrale Instanz oder eine stark reduzierte Anzahl an Teilnehmern gewährt.[146]

Unabhängig vom gewählten Ansatz lassen sich Blockchains zudem hinsichtlich ihres Anwendungsgebietes systematisieren. Dabei wird häufig zwischen drei Generationen unterschieden, welche an dieser Stelle kurz erläutert werden.

- **Blockchain 1.0**
  Zu Blockchains der ersten Generation werden Distributed-Ledger-Systeme gezählt, die ausschließlich zum Transfer von virtuellen Währungen (Kryptotokens) genutzt werden.[147]
- **Blockchain 2.0**
  Die zweite Generation dehnt den Funktionsumfang der DLT auf weitere wirtschaftliche Anwendungsbereiche aus. Diese Blockchains sollen mithilfe selbstausführender Verträge, sog. Smart Contracts auch komplexe Finanzinstrumente, wie z. B. Aktien, Anleihen und Termingeschäfte abbilden und hierdurch die Vorteile der DLT auf weitere finanzwirtschaftliche Anwendungsgebiete übertragen können.[148]
- **Blockchain 3.0**
  Zu Blockchains der dritten und neuesten Generation werden sämtliche DLT-Systeme gezählt deren Anwendungsbereich außerhalb der Finanzwirtschaft liegt. Hierzu zählen beispielsweise Anwendungen im Gesundheitsweisen oder dem künstlerischen Bereich.[149]

Im Hinblick auf die Zielsetzung der vorliegenden Masterarbeit werden im weiteren Untersuchungsverlauf ausschließlich Blockchains der ersten und zweiten Generation näher betrachtet, welche sich entweder dem öffentlichen oder dem privaten Blockchain-Ansatz zuordnen lassen. Im nächsten Abschnitt werden ausgewählte Praxisbeispiele für beide Ansätze überblicksartig vorgestellt. Diese werden im Rahmen der darauffolgenden Untersuchung auf ihre Stärken und Schwächen hin untersucht.

3.1.2 Untersuchte Blockchains

Das bekannteste Praxisbeispiel für eine öffentliche Blockchain ist **Bitcoin.** Einige Elemente dieser Blockchain sind bereits zur Erklärung der theoretischen Grundlagen beschrieben worden. Um dem Leser der vorliegenden Masterarbeit aber ein vollständiges Bild hinsichtlich der Zielsetzung und der Eigenschaften von Bitcoin zu ermöglichen erfolgt an dieser Stelle eine Kurzdarstellung der Bitcoin-Blockchain. Wie bei allen öffentlichen Blockchains ist Bitcoins gesamte Transaktionshistorie bis zum ersten aufgezeichneten Block, dem sog. Genesis Block,

[145] Vgl. BaFin (2017).
[146] Vgl. BaFin (2017).
[147] Vgl. Swan (2015), S. ix.
[148] Vgl. Efanov/Roschin (2018), S. 117 f.
[149] Vgl. Efanov/Roschin (2018), S. 118.

öffentlich einsehbar.[150] Hierzu kann entweder die Full-Node-Software installiert[151] oder ein spezialisierter Online-Dienst verwendet werden.[152] Bitcoin ist als Alternative zum aktuellen Zahlungssystem entwickelt worden[153] und nutzt zur Wertübertragung und zur Entlohnung der Full-Nodes die gleichnamige native Kryptowährung Bitcoin (BTC).[154] Zur Bestätigung von Transaktionen und zur Konsensbildung wird ein Proof-of-Work-Konsensprotokoll verwendet.[155] Bitcoin hat zum Zeitpunkt der Bearbeitung vorliegender Masterarbeit eine geschätzte Marktkapitalisierung von mehr als 117 Milliarden Euro.[156]

Die höchste geschätzte Marktkapitalisierung nach Bitcoin hat die ebenfalls öffentliche Blockchain **Ethereum**. Diese betrug im März 2018 ca. 49 Milliarden Euro.[157] Wie auch bei Bitcoin ist die Transaktionshistorie dieser Blockchain öffentlich einsehbar.[158] Eine weitere Gemeinsamkeit der beiden Blockchains ist die Verwendung einer nativen Kryptowährung, welche im Fall von Ethereum als Ether (ETH) bezeichnet wird.[159] Diese wird als Transaktionsmedium, aber auch als Entlohnungselement für die Miner des Netzwerks verwendet.[160] Ethereum setzt derzeit wie auch Bitcoin auf ein PoW-Protokoll zur Validierung der Transaktionen.[161] Ethereum wird den Blockchains der 2. Generation (Blockchain 2.0) zugeordnet, da neben der Durchführung und Aufzeichnung simpler Transaktionen auch komplexe Smart Contrats möglich sind.[162]

Als Beispiel für eine private Blockchain kann **Ripple** angeführt werden.[163] Es ist jedoch anzumerken, dass es sich bei Ripple nicht um eine vollständig private Blockchain handelt, sondern um eine Hybridlösung,[164] welche aufgrund der Definition im vorangegangenen Abschnitt dem Private-Blockchain-Ansatz zugeordnet wird.[165] Wie auch die öffentlichen Blockchains verwendet Ripple eine eigene Kryptowährung namens Ripple (XRP).[166]Anders als in den öffentlichen Blockchains versucht Ripple allerdings nicht Finanzintermediäre durch ein dezentrales Transaktionssystem zu ersetzen, sondern bindet gezielt Banken und andere Finanzinstitutionen in die eigene Blockchain-Ökosphäre ein, um ein neues weltumfassendes Zahlungsprotokoll aufzubauen.[167] Ripple bietet dabei verschiedene Blockchain-Plattformen an, welche jeweils an unterschiedliche Arten von Finanzdienstleistern adressiert sind. Im Rahmen dieser Untersuchung wird allerdings ausschließlich die Plattform **xCurrent** betrachtet. Hierbei handelt es sich um eine speziell auf den Zahlungsverkehr zwischen Banken ausgerichtete Plattform, welche ein

[150] Vgl. SIXT (2017), S. 40.
[151] Vgl. SIXT (2017), S. 40.
[152] Vgl. SWAN (2015), S. x.
[153] Vgl. SEITZ (2016), S. 165 f.
[154] Vgl. BURGWINKEL (2016), S. 9.
[155] Vgl. NAKAMOTO (2008), S. 3.
[156] Vgl. Coinmarketcap (2018), Stand am 16.03.2018.
[157] Vgl. Coinmarketcap (2018), Stand am 16.03.2018.
[158] Vgl. BaFin (2017).
[159] Vgl. BRÜHL (2017a), S. 13.
[160] Vgl. BURGWINKEL (2016), S. 9.
[161] Vgl. FREUND (2017), S. 69.
[162] Vgl. SEITZ (2016), S. 174.
[163] Vgl. METI (2016), S. 31.
[164] Vgl. MORABITO (2017), S. 9.
[165] Vgl. Abschnitt 3.1.1.
[166] Vgl. ROSNER/KANG (2016), S. 659.
[167] Vgl. PILKINGTON (2016), S. 241 f.

spezielles Protokoll zur Erfassung von Transaktionsdaten nutzt und hierdurch eine, auf die Bedürfnisse von Banken angepasste, Blockchain-Lösung schaffen soll.[168]

Als letztes Untersuchungsobjekt dient **Hyperledger.** Hierbei handelt es sich nicht um ein spezifisches Netzwerk, sondern um ein modulares Gerüst zur Erstellung von individuellen Blockchains.[169] In den aktuellen Versionen ist Hyperledger stets auf die Erstellung privater Blockchains in einem teilweise vertrauensbasierten Netzwerk ausgerichtet.[170] Hyperledger gilt aufgrund einer hohen Leistungsfähigkeit als vielversprechende Blockchain-Plattform[171] und wird von führenden Finanzdienstleistern, wie z. B. Society for Worldwide Interbank Financial Telecommunication (SWIFT) zur Entwicklung eigener Blockchain-Lösungen verwendet.[172] Aber auch die Europäische Zentralbank (EZB) testet zusammen mit der Bank of Japan (BOJ) innerhalb des „Project Stella" die Anwendungsmöglichkeiten der Hyperledger-Plattform zur Effizienzsteigerung von Finanztransaktionen.[173] Im Rahmen der Untersuchung wird zur Beurteilung der Hyperledger-Blockchain hauptsächlich die Konfiguration des Project Stella der EZB und BOJ betrachtet. Hierbei handelt es sich um die Hyperledger-Plattform **Fabric**,[174] welche in einem Test-Netzwerk zur Abbildung von Interbankenzahlungen verwendet wird.[175] Weitere Details der Untersuchung werden im nachfolgenden Abschnitt genauer beschrieben.

3.2 Untersuchungsaufbau

Gemäß der Zielstellung der vorliegenden Arbeit sollen der Private- und der Public-Blockchain-Ansatz miteinander verglichen werden. Hierzu bietet sich die Stärken-Schwächen-Analyse als Untersuchungsinstrument an. Bei der **Stärken-Schwächen-Analyse** handelt es sich um ein Instrument aus dem Bereich der strategischen Unternehmenssteuerung, bei dem strategische Potenziale eines Unternehmens ermittelt und bewertet werden sollen.[176] Zur Bewertung werden aus den Potenzialen kritische Erfolgsfaktoren abgeleitet deren jeweilige Ausprägung spezifische Stärken, bzw. Schwächen eines Unternehmens darstellen.[177]

Parallel zur Untersuchung des eigenen Unternehmens sollte auch ein Profil des stärksten Konkurrenten ermittelt werden. Hierdurch wird die interne Analyse des eigenen Unternehmens um eine externe Komponente erweitert und so die Aussagekraft der Ergebnisse erhöht.[178] Zur Visualisierung der Merkmalsausprägung wird ein Stärken-Schwächen-Profil beider Untersuchungsobjekte erstellt, welches einen direkten Vergleich beider Unternehmen und somit die Identifikation von Wettbewerbsvorteilen ermöglicht.[179] Ein Beispiel hierfür ist in der nachfolgenden Abbildung 6 zu sehen.

---

[168] Vgl. Ripple (2017), S. 4.
[169] Vgl. Hyperledger (2017), S. 3.
[170] Vgl. Hyperledger (2017), S. 4.
[171] Vgl. Ploom (2016), S. 140.
[172] Vgl. Formann (2017), S. 38.
[173] Vgl. EZB/BOJ (2017), S. 2-4.
[174] Vgl. EZB/BOJ (2017), S. 4.
[175] Vgl. EZB/BOJ (2017), S. 14.
[176] Vgl. Baum/Coenenberg/Günther (2007), S. 71.
[177] Vgl. Bea/Haas (2017), S. 129 f.
[178] Vgl. Baum/Coenenberg/Günther (2007), S. 71.
[179] Vgl. Horváth (2012), S. 330.

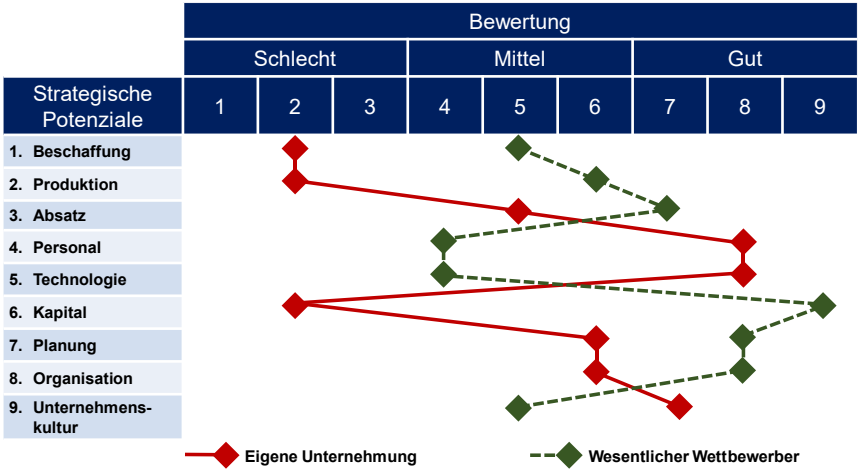


Abbildung 6: Beispiel für ein Stärken-Schwächen-Profil zweier Unternehmen[180]

Statt strategischer Potenziale, können die kritischen Erfolgsfaktoren jedoch auch direkt zum Aufbau des eigenen Stärken-Schwächen-Profils verwendet werden.[181] Dieses Vorgehen wird auch zum Vergleich der beiden Blockchain-Ansätze verwendet. Hierbei muss jedoch berücksichtigt werden, dass viele Elemente der Blockchain in wechselseitiger Beziehung zueinander stehen. So wirkt sich beispielsweise das gewählte Zugangs- und Transparenzmodell stark auf die Wahl des Konsensmechanismus aus,[182] welcher wiederum u. a. die Sicherheit, und die Effizienz der Blockchain beeinflusst.[183]

Um dennoch eine möglichst differenzierte Betrachtung der Stärken und Schwächen beider Ansätze zu ermöglichen, wurde die Analyse in zwei Untersuchungsteile aufgeteilt. Im ersten Untersuchungsteil werden kritische Erfolgsfaktoren der Blockchain, welche einen direkten Bezug zum **Zugangs- und Transparenzmodell** aufweisen, betrachtet. Der Fokus des zweiten Untersuchungsteils hingegen liegt auf Erfolgsfaktoren, welche direkt vom **Konsensmechanismus** beeinfluss werden. Die Beurteilungskriterien werden dabei zu Beginn der Analyse jedes Erfolgsfaktors separat definiert. Sie lassen sich jedoch stets einer der zwei folgenden Kategorien zuordnen.

- **Erfolgsfaktor mit Zielvorgabe:**
  Existiert zur Bewertung eines Erfolgsfaktors eine spezifische Zielvorgabe, wie z. B. die Erfüllung regulatorischer Vorgaben, gilt eine ausreichende Erfüllung dieses Zielwerts als Stärke. Ein Nichterfüllen wird dementsprechend als Schwäche gewertet.

[180] Quelle: Eigene Darstellung, in Anlehnung an Bea/Haas (2017), S. 132.
[181] Vgl. Bea/Haas (2017), S. 132.
[182] Vgl. Pinna/Ruttenberg (2016), S. 11 f.
[183] Vgl. Vukolić (2016), S. 115.

- **Erfolgsfaktoren ohne Zielvorgabe:**
  Bei der Beurteilung bestimmter Erfolgsfaktoren, exemplarisch sei hier auf den möglichen Redundanzgrad eines Blockchain-Ansatzes verwiesen, konnte im Rahmen der Literaturrecherche keine Zielvorgabe ermittelt werden. Dementsprechend wird bei der Analyse dieser Faktoren zu Beginn des Untersuchungsabschnitts zunächst erläutert, ob eine hohe, bzw. niedrige Merkmalsausprägung der Beurteilungskriterien als Vor-, bzw. Nachteil anzusehen ist.

Nach der Untersuchung der kritischen Erfolgsfaktoren, werden die Ergebnisse in einem Stärken-Schwächen-Profil visualisiert. Dieses weicht jedoch von dem in der Abbildung 6 dargestellten Verfahren ab, da keine ordinale Punkteskala verwendet wird. Diese bietet zwar den Vorteil, dass neben einer absoluten Einschätzung der eigenen Stärken und Schwächen auch relative Stärken und Schwächen gegenüber einem Konkurrenten ermittelt werden können,[184] gleichzeitig weist das Verfahren aber auch Defizite auf. Laut WÖHE/DÖRING stellt insbesondere die Subjektivität bei der Bewertung der Merkmalsausprägung ein Problem der Stärken-Schwächen-Analyse dar, da in der Mehrzahl der Fälle keine quantifizierbare Größe zur Messung der Merkmalsausprägung gefunden werden kann.[185]

Dieses Problem ist auch bei der Beurteilung von Stärken und Schwächen der untersuchten Blockchain-Ansätze anzutreffen. Es konnte in vielen Bereichen, beispielhaft sei hier auf die Beurteilung der Manipulationsresistenz verwiesen, keine sinnvolle Metrik zur Einordnung eines Ansatzes entlang einer Skala gefunden werden. Dementsprechend wird eine simple Stärken-Schwächen-Matrix ohne Punkteskala verwendet. Dabei wird für jeden Erfolgsfaktor festgestellt, ob dieser eine Stärke oder eine Schwäche des jeweiligen Ansatzes darstellt. Sollte weder eine Einstufung als Stärke, noch als Schwäche möglich sein, wird betreffender Ansatz in der Kategorie „keine Aussage möglich“ eingeordnet. Ein Beispiel hierfür stellt Tabelle 4 dar.

Untersuchte Faktoren	Stärke	Keine Aussage möglich	Schwäche
Untersuchungsteil 1			
- Erfolgsfaktor 1			
- Erfolgsfaktor 2			
- …			
Untersuchungsteil 2			
- Erfolgsfaktor 1			
- …			

Tabelle 4: Aufbau des Stärken-Schwächen-Profils[186]

[184] Vgl. BAUM/COENENBERG/GÜNTHER (2007), S. 73.
[185] Vgl. WÖHE/DÖRING (2010), S. 87.
[186] Quelle: Eigene Darstellung, in Anlehnung an BEA/HAAS (2017), S. 132.

Zur Beurteilung der Ansätze stützt sich die Analyse auf bisherige Forschungserkenntnisse zur Ausprägung der jeweiligen Erfolgsfaktoren beim Private- und beim Public-Blockchain-Ansatz. Da es sich bei der DLT um eine junge Technologie handelt, welche sich weitestgehend noch in einem experimentellen Entwicklungsstadium befindet,[187] sind aktuell lediglich zu wenigen potenziellen Anwendungsmöglichkeiten und kritischen Erfolgsfaktoren unabhängige wissenschaftliche Untersuchungen verfügbar.[188] Dementsprechend können einige kritische Erfolgsfaktoren von Blockchains, wie z. B. die Nutzung von Smart Contracts, in den nachfolgenden beiden Untersuchungsteilen nicht berücksichtigt werden.

3.3 Untersuchungsteil I: Zugangs- und Transparenzmodell

Das erste Untersuchungsgebiet ist das Zugangs- und Transparenzmodell der beiden Blockchain-Ansätze. Dieses unterscheidet sich, wie bereits bei der Systematisierung der Blockchain-Ansätze erläutert, deutlich voneinander.[189] Während in öffentlichen Blockchains jeder Akteur ohne Einschränkungen Zugang zur Blockchain hat und sämtliche Transaktionsdaten einsehen kann,[190] sind Zugang sowie Lese- und Schreiberechte in privaten Blockchains beschränkt.[191] Auch hinsichtlich der Identität der Netzwerkteilnehmer unterscheiden sich beide Blockchain-Ansätze signifikant voneinander. In privaten Netzwerken wie Ripple müssen sich alle Teilnehmer über zentrale Intermediäre, sog. Gateways, identifizieren.[192] In öffentlichen Blockchains erfolgt keine verpflichtende Identitätsfeststellung, stattdessen kann jeder Nutzer selbst bestimmen, wie viele Informationen er bezüglich seiner Identität mit den restlichen Netzwerkteilnehmern teilen möchte.[193] Zudem sind zentrale Intermediäre in öffentlichen Blockchains nicht vorgesehen, da diese mit dem Ziel der Entfernung von Intermediären entwickelt wurden.[194] In den weiteren Abschnitten dieses Untersuchungsteils soll festgestellt werden, welche Auswirkungen die gegensätzlichen Zugangs- und Transparenzmodelle auf die kritischen Erfolgsfaktoren Schutz sensibler Daten, Sicherheit zentraler Intermediäre und Flexibilität bei der Wahl des Konsensmechanismus haben.

3.3.1 Schutz sensibler Daten

Befürworter öffentlicher Blockchains kritisieren das aktuelle Zahlungssystem dahingehend, dass z. B. bei der Nutzung von Kreditkarten sämtliche Zahlungsdaten des Zahlenden für den Transaktionspartner einsehbar sind und somit von diesem beispielsweise zu Analysezwecken genutzt werden können. Um dem zu entgehen müssen aktuell Intermediäre wie z. B. Paypal genutzt werden, dies ist allerdings mit zusätzlichen Kosten verbunden.[195] Mithilfe der DLT soll ein höherer Schutz vertraulicher Finanzdaten ermöglicht werden, hierzu verfolgen jedoch beide

[187] Vgl. TOBIAS (2016), S. 39; vgl. SWIFT (2016), S. 14.
[188] Vgl. YLI-HUUMO ET AL. (2016), S. 19-22.
[189] Vgl. Abschnitt 3.1.1.
[190] Vgl. PILKINGTON (2016), S. 230 f.
[191] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 42 f.
[192] Vgl. SIXT (2017), S. 181.
[193] Vgl. SIXT (2017), S. 155.
[194] Vgl. SEITZ (2016), S. 166.
[195] Vgl. SIXT (2017), S. 155.

Blockchain-Ansätze unterschiedliche Vorgehensweisen. Im Nachfolgenden soll daher untersucht werden, inwieweit der Schutz vertraulicher Finanzdaten als Stärke oder Schwäche des jeweiligen Ansatzes gewertet werden kann.

Ein zentraler Bestandteil öffentlicher Blockchains ist, dass einzelne Transaktionen sowie die vollständige Transaktionshistorie jederzeit einsehbar sind, da diese zur Bestätigung alle Transaktionen öffentlich zwischen den validierenden Nodes kommuniziert werden müssen.[196] Dementsprechend lassen sich alle bestätigten Transaktionen bis zum Beginn der Aufzeichnungen zurückverfolgen.[197] Hieraus ergibt sich eine sehr hohe Transparenz der Transaktionsdaten, welche im Hinblick auf den Datenschutz äußert bedenklich einzustufen ist. Denn mithilfe von Finanzdaten lassen sich Rückschlüsse auf die persönlichen Gewohnheiten und Lebensumstände von Privatpersonen ziehen.[198]

Aber auch für Unternehmen ist die hohe Transparenz öffentlicher Blockchains nachteilig zu bewerten. Beispielsweise könnten Handelsstrategien von Wertpapierhändlern identifiziert werden, wodurch Wettbewerber entsprechende Konterstrategien entwickeln könnten.[199] Statt realer Personal-, bzw. Unternehmensdaten sehen öffentliche Blockchains dementsprechend die Nutzung zufallsgenerierter Adressen als Identität im Netzwerk vor. Laut NAKAMOTO sei hierdurch eine Anonymisierung der Nutzer trotz öffentlicher Transaktionshistorie möglich. Als zusätzlicher Sicherheitsmechanismus dient die Möglichkeit ständig neue Adressen erzeugen zu können.[200] Bitcoins Modell zur Erfassung von Vermögenswerten namens **Unspent Transactions Output (UTXO)** unterstützt diese Anonymisierung, da Bitcoins Transaktionshistorie keine Kontostände erfasst, sondern anhand der In- und Outputs von Transaktionen einen virtuellen Kontostand pro Akteur ermittelt.[201]

Zur Verdeutlichung der Systematik dient folgendes Beispiel. Der Akteur „Alice“ kauft einen Gegenstand vom Verkäufer „Bob“ zum Preis von 0,05 Bitcoin. Alice nutzt hierzu das Vermögen auf einer in ihrem Wallet gespeicherten Adressen. Auf der gewählten Adresse sind 0,12 Bitcoin hinterlegt. Da UTXO keine teilweisen Zahlungen unterstützt, muss Alice den gesamten Betrag als Transaktionsinput wählen.[202] Als Output wählt sie einerseits 0,05 Bitcoin, welche an Bobs Adresse versendet werden und 0,07 Bitcoin, welche an eine ihrer Adressen versendet werden. In beiden Fällen kann eine völlig neu erstellte Adresse als Zieladresse fungieren.[203] Dieses Beispiel ist in Abbildung 7 grafisch dargestellt.

---

[196] Vgl. NAKAMOTO (2008), S. 6.
[197] Vgl. NARAYANAN ET AL. (2016), S. 139.
[198] Vgl. BÖHME/PESCH (2017), S. 473.
[199] Vgl. PLOOM (2016), S. 143.
[200] Vgl. NAKAMOTO (2008), S. 6; vgl. DUPONT/SQUICCIARINI (2015), S. 139; vgl. LI ET AL. (2017), S. 6.
[201] Vgl. KIENZLER (2016), S. 119; vgl. PINNA/RUTTENBERG (2016), S. 16.
[202] Vgl. PINNA/RUTTENBERG (2016), S. 16.
[203] Vgl. BOLESCH/MITSCHELE (2016), S. 36.

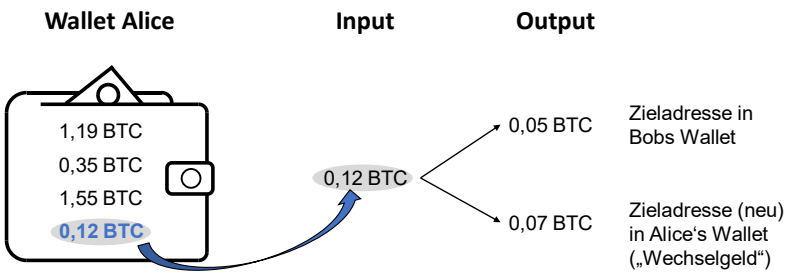


Abbildung 7: Funktionsweise des UTXO-Modells zur Asseterfassung[204]

Ethereum hingegen verwendet ein Account-Modell. Diese Art der Vermögenserfassung ermöglicht es Veränderungen des Kontostandes auf der Blockchain zu erfassen.[205] Wie bei allen öffentlichen Blockchains können auch hier verschiedene Identitäten genutzt werden.[206] Trotz der Verschleierung durch die Nutzung mehrerer Identitäten (Adressen, bzw. Accounts) bieten öffentliche Blockchains keine wirkliche Anonymität, sondern vielmehr eine **Pseudonymität**, da zwar keine realen Identitäten verwendet werden, jede Transaktion sich jedoch zu bestimmten Adressen und somit zu bestimmten Pseudonymen zuordnen lässt.[207]

Zum Schutz der Privatsphäre muss dementsprechend eine Verknüpfung der Transaktionen mit den dazugehörigen real existierenden Personen, Unternehmen und Institutionen verhindert werden, da sonst sämtliche vergangenen, aktuellen aber auch zukünftigen Transaktionen für jedermann einsehbar und interpretierbar wären.[208] Es gibt zahlreiche Beispiele für erfolgreiche Verknüpfungen realer Personen mit ihren Pseudonymen auf der Bitcoin Blockchain. AL JAWAHERI ET AL. konnten beispielsweise durch eine Analyse der Nutzerdaten in sozialen Netzwerken und Onlineforen zahlreiche Nutzer mit Bitcoin-Adressen, welche zur Nutzung versteckter Dienste im Internet verwendet wurden, in Verbindung bringen. [209] Aber auch Strafverfolgungsbehörden konnten bereits in mehreren Fällen Drogenhändler, Geldwäscher und andere Kriminelle erfolgreich identifizieren.[210] Die Verknüpfung realer Identitäten mit den Pseudonymen stellt jedoch auch für nicht kriminelle Nutzer öffentlicher Blockchains ein schwerwiegendes Sicherheitsproblem dar. Denn mit der Zuordnung einer Adresse können nicht nur vergangene, sondern auch zukünftige Transaktionen dieser Adresse öffentlich eingesehen werden.[211]

Zur Lösung dieses Problems nutzen Akteure öffentlicher Blockchains unterschiedliche Methoden, wie z. B. die Anonymisierung der eigenen Internet-Protokoll-Adresse (IP-Adresse) mithilfe von Virtual-Private-Network-Diensten (VPN-Dienst) oder die Verschleierung der eigenen Transaktionshistorie durch die Nutzung von Mixer-Diensten. Die Notwendigkeit zur Verschleierung der eigenen IP-Adresse ist dem dezentralen Netzwerkaufbau öffentlicher Blockchains

[204] Quelle: Eigene Darstellung, in Anlehnung an BOLESCH/MITSCHELE (2016), S. 36.
[205] Vgl. GREENSPAN (2016), 176 f.
[206] Vgl. PINNA/RUTTENBERG (2016), S. 12.
[207] Vgl. NARAYANAN ET AL. (2016), S. 139; vgl. BÖHME ET AL. (2015), S. 228 f.
[208] Vgl. NARAYANAN ET AL. (2016), S. 141; vgl. KIENZLER (2016), S. 112.
[209] Vgl. AL JAWAHERI ET AL. (2018), S. 10
[210] Vgl. YERMACK (2017), S. 18.
[211] Vgl. NARAYANAN ET AL. (2016), S. 139.

geschuldet. Da Blockchains P2P-Systeme sind, lässt sich durch eine Analyse der Transaktionskaskade feststellen, von welchem Gerät eine bestimmte Transaktion initiiert wurde. Hierdurch lässt sich die IP-Adresse des Initiators einer Transaktion feststellen, welche ggf. Rückschlüsse auf dessen Identität ermöglicht.[212] Um dies erfolgreich bewerkstelligen zu können, muss ein Angreifer zwar einen Großteil des Netzwerks überwachen können, dies ist aber beispielsweise bei Bitcoin bereits mit einem geringen Budget möglich.[213]

Durch die Nutzung eines VPN-Dienstes können Nutzer ihre eigene IP-Adresse verschleiern und erhalten so einen gewissen Schutz vor der Enttarnung durch eine Analyse des Informationsflusses.[214] Doch auch die Verschleierung der IP-Adresse bietet keine vollständige Verschleierung der persönlichen Daten. So konnten z. B. Bitcoin-Transaktionen anhand der Uhrzeiten zum Zeitpunkt der Transaktionsinitiierung bestimmten geografischen Regionen zugeordnet werden. DUPONT/SQUICCIARINI werten dies als ersten Schritt zur Enttarnung von Nutzern.[215] Auch NARAYANAN ET AL. sehen langfristig ein steigendes Risiko der Deanonymisierung von Nutzern öffentlicher Blockchains, da die historische Entwicklung von Algorithmen zur Deanonymisierung einen stetigen Anstieg der Erfolgswahrscheinlichkeit mit zunehmendem Zeitverlauf zeigt.[216]

Neben einer Verschleierung der IP-Adresse können Akteure auf öffentlichen Blockchains auch ihre eigene Transaktionshistorie verschleiern, indem sie auf sog. Mixer-Dienste zurückgreifen. Dieses Konzept geht zurück auf CHAUM, welcher einen Dienst zur Verschleierung der Kommunikationsbeziehungen in öffentlichen Netzwerken vorschlug. In diesem Konzept sollten E-Mails von den einzelnen Netzwerkteilnehmern gesammelt und anschließend stapelweise an die entsprechenden Empfänger gesendet werden.[217] Dieses Verfahren ist auch in den öffentlichen Blockchains möglich. Hierbei werden Kryptotokens anstelle von E-Mails zunächst an einen Mixer-Dienst gesendet. Dieser sendet nun die erhaltenen Kryptotokens über zusätzliche Zwischenstellen hinweg an den gewünschten Empfänger weiter und verschleiert hierdurch die Transaktionsbeziehung zwischen ursprünglichem Sender und finalem Empfänger.[218]

Dabei ist die Effektivität stark von der Kundenbasis des Mixing-Dienstes abhängig, wie z. B. eine Untersuchung von MÖSER/BÖHME/BREUKER zeigt. In dieser konnte festgestellt werden, dass einige Mixer, welche gleichzeitig auch Online-Wallet-Anbieter waren, die Enttarnung einzelner Nutzer signifikant erschweren. Bei anderen Diensten hingegen war in zwei Dritteln aller Experimente eine Verknüpfung des Inputs und Outputs nach dem Mixingvorgang möglich.[219] Neben der unterschiedlichen Qualität der Dienste lassen sich zwei weitere negative Eigenschaften von Mixer-Diensten feststellen. Zum einen ist die Anonymisierung mithilfe von Mixing-

[212] Vgl. PETRLIC/SORGE (2017), S. 84; vgl. SIXT (2017), S. 155.
[213] Vgl. PETRLIC/SORGE (2017), S. 84 f.
[214] Vgl. PETRLIC/SORGE (2017), S. 25.
[215] Vgl. DUPONT/SQUICCIARINI (2015), S. 140 f.
[216] Vgl. NARAYANAN ET AL. (2016), S. 149.
[217] Vgl. PETRLIC/SORGE (2017), S. 49 f.
[218] Vgl. BÖHME ET AL. (2015), S. 221.
[219] Vgl. MÖSER/BÖHME/BREUKER (2013), S. 10.

Diensten mit zusätzlichen Transaktionskosten verbunden, welche zwischen einem und drei Prozent der Transaktionssumme betragen können. Zum anderen besteht die Gefahr, dass kriminelle gezielt Mixing-Dienste anbieten und die hierdurch erhaltenen Kryptotokens stehlen.[220]

Private Blockchains, wie Ripple und Hyperledger verfolgen hinsichtlich der Transparenz der Transaktionsdaten und der Identifizierbarkeit der Teilnehmer eine völlig andere Zielsetzung als ihre öffentlichen Pendants. In privaten Blockchains müssen sich sämtliche Teilnehmer identifizieren, um im Netzwerk mitwirken zu können.[221] Zum Schutz vertraulicher Daten, wie z. B. der persönlichen Daten oder der Handelsstrategie eines Nutzers kann jedoch die Einsehbarkeit der Daten auf einen ausgewählten Kreis an Akteuren beschränkt werden. Bei Hyperledger ist es z. B. möglich vollständig geschlossene Blockchains zu erstellen.[222] Außerdem können auch sog. Subledger genutzt werden, welche Transaktionen zwischen einzelnen Teilnehmern ermöglichen, ohne die Transaktionsdetails anderen Netzwerkteilnehmern zugänglich zu machen.[223] Dabei können in bestimmten Intervallen Referenzwerte zu Transaktionen auf den öffentlichen Ledger gespeichert werden.[224]

Auch Ripple nutzt Subledger im Rahmen des **Interledger-Protokolls (ILP)** um trotz eines übergeordneten öffentlich einsehbaren Hauptledgers, dem sog. Ripple Consensus Ledger (RCL), diskrete Transaktionen zwischen einzelnen Netzwerkteilnehmern zu ermöglichen.[225] Zusätzlich unterscheidet sich Ripple dahingehend von öffentlichen Blockchains, dass in der xCurrent-Plattform Privatnutzer und Unternehmen keine direkten Akteure der privaten Blockchain darstellen, sondern sämtlichen Zahlungsverkehr über Banken als Intermediäre abwickeln.[226] Hierdurch entsteht in der privaten Blockchain ein völlig anderer Informationsfluss als in den öffentlichen Netzwerken. Zur Verdeutlichung sei hier erneut die zuvor benutzte Beispieltransaktion zwischen Alice und Bob verwendet. Alice möchte einen Gegenstand von Bob kaufen. Die Zahlung des Kaufbetrags wird jedoch nicht direkt zwischen den beiden Transaktionspartner abgewickelt, stattdessen nutzen beide hierzu ihre Bank als Intermediär.[227] Der Informationsfluss ist in der nachfolgenden Abbildung 8 grafisch dargestellt.

[220] Vgl. Böhme et al. (2015), S. 221 f.
[221] Vgl. Seitz (2016), S. 176; vgl. Pinna/Ruttenberg (2016), S. 11; vgl. Vukolić (2016), S. 116.
[222] Vgl. Kienzler (2016), S. 112 f.
[223] Vgl. Gramoli (2017), S. 9.
[224] Vgl. Yermack (2017), S. 16.
[225] Vgl. Liu (2015).
[226] Vgl. Ripple (2017), S. 6.
[227] Vgl. Ripple (2017), S. 6.

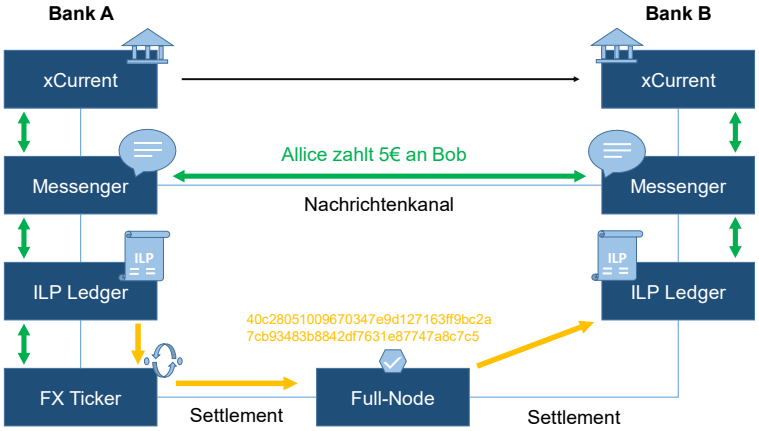


Abbildung 8: Informationsfluss in xCurrent[228]

Die Übermittelten Informationen lassen sich dabei in zwei Ebenen unterteilen. In Ebene 1 (grün) wird eine direkte Nachrichtenverbindung zwischen den beiden an der Transaktion beteiligten Banken über die **Messenger-Funktion** eröffnet. In der Abbildung 8 wird dies durch die grünen Pfeile dargestellt. Hierdurch können die beteiligten Intermediäre sämtliche, zur Durchführung der Transaktion benötigten, Informationen in einem direkten Informationskanal austauschen und abgleichen. Dies ermöglicht u.a. die Prüfung, ob es sich um Kunden der jeweiligen Bank handelt und ob der Initiator der Zahlung (Alice) über ausreichende Mittel verfügt. Sind die benötigten Informationen übermittelt und auf ihre Gültigkeit überprüft worden, werden die benötigten Geldmittel, also der zu überweisende Betrag zusätzlich der Transaktionsgebühren auf dem ILP-Ledger von Bank A und B eingefroren.[229]

Anschließend erfolgt der Informationsfluss auf der verschlüsselten Ebene 2, welche in der Abbildung 8 gelb dargestellt wird. Bank A und B übermitteln jeweils einen kryptografischen Nachweis darüber, dass die Transaktion im ILP erfasst wurde an die Full-Nodes des Ripple-Netzwerkes. Persönlichen Daten der Transaktionspartner Alice und Bob sowie die Details der Transaktion werden hierbei nicht übermittelt und sind folglich weder für die Full-Nodes, noch für andere Netzwerkteilnehmer einsehbar.[230] Haben die Full-Nodes beide Nachweise erhalten, leiten sie das Settlement ein. Hierdurch werden die Bilanzen der beiden Banken aktualisiert und die zuvor eingefrorenen Geldmittel wieder freigegeben.[231]

Im Hinblick auf den Datenschutz ist der vollständig transparente Ansatz öffentlicher Blockchains als Schwäche zu bewerten. Es konnten mehrere Methoden zur Deanonymisierung von Akteuren nachgewiesen werden. Zudem ist davon auszugehen, dass diese Methoden langfristig effektiver werden.[232] Als zentraler Schwachpunkt des öffentlichen Ansatzes kann die direkte

[228] Quelle: Eigene Darstellung, in Anlehnung an Ripple (2017), S. 4.
[229] Vgl. Ripple (2017), S. 8.
[230] Vgl. Ripple (2017), S. 8.
[231] Vgl. Ripple (2017), S. 9.
[232] Vgl. NARAYANAN ET AL. (2016), S. 149.

Verknüpfung von Accounts, bzw. Adressen der Akteure mit einer spezifischen Transaktion genannt werden. Die Verknüpfung kann zwar beispielsweise durch die Nutzung spezialisierter Mixing-Dienste aufgehoben werden, diese sind jedoch nicht immer erfolgreich und mit zusätzlichen Kosten verbunden. Diese ist durch die Nutzung zentraler Intermediäre in privaten Blockchains nicht vorhanden. Hierzu sei auf die beispielhafte Transaktion innerhalb des Ripple-Netzwerkes verwiesen. Die Full-Nodes haben zwar von den Intermediären der beiden Unternehmen Informationen erhalten, hierbei handelte es sich jedoch ausschließlich um kryptografische Nachweise zur Einigung auf eine Transaktion. Deren Details sind nicht öffentlich einsehbar und somit lässt eine Auswertung des Informationsflusses zwischen den beteiligten Banken und den Validator-Nodes keine Rückschlüsse auf eine Transaktion zwischen den Akteuren Alice und Bob zu.[233] Zusammenfassend kann somit festgestellt werden, dass private Blockchains hinsichtlich des Schutzes privater Daten den öffentlichen Blockchains eindeutig vorzuziehen sind.

3.3.2 Sicherheit zentraler Intermediäre

Grundsätzlich benötigen öffentliche Blockchains keine Intermediäre, denn mithilfe eines Wallets können in öffentlichen Blockchains Transaktionen direkt zwischen den Netzwerkteilnehmern getätigt werden.[234] Mit der Nutzung unterschiedlicher Wallet-Typen sind jedoch auch Risiken verbunden. Bei Nutzung eines Offline-Wallets, ist beispielsweise keine Wiederherstellung des Private Keys möglich, sofern dieser verloren oder vernichtet wurde, da keine zentrale Institution vorhanden ist, die über entsprechende Möglichkeiten verfügt.[235] Sämtliche auf dieses Schlüsselpaar transferierten Mengen der Kryptowährung sind somit unwiederbringlich verloren.[236] Selbiges gilt i. d. R. auch für den Fall, dass der private Schlüssel infolge eines Hackerangriffs gestohlen wird.[237]

Aufgrund dieser Risiken verwenden zunehmend mehr Bitcoin-Nutzer Online Wallets spezialisierter **Wallet-Anbieter.** Neben der Aufbewahrung der privaten Schlüssel fungieren viele Wallet-Anbieter, wie z. B. Mt. Gox oder Bitfinex auch als Schnittstelle zwischen der virtuellen Kryptoökonomie öffentlicher Blockchains und der Realwirtschaft, indem sie einen Tausch gesetzlicher Zahlungsmittel in die Kryptowährungen öffentlicher Blockchains ermöglichen.[238] Diese Art von Wallet-Anbietern wird auch als **Kryptowährungsbörse** bezeichnet.[239] Mit einer Ausweitung des Funktionsumfangs tragen Wallet-Anbieter allerdings zu einer zunehmenden Zentralisierung öffentlicher Blockchains bei.[240] Einen Nachweis hierfür liefert eine Studie von MEIKLEJOHN ET AL. Diese untersuchten mithilfe heuristischer Verfahren den Transaktionsfluss innerhalb des Bitcoin-Netzwerks und konnten dabei feststellen, dass ein Großteil der Transaktionen über bestimmte Dienste abgewickelt wird.[241] Die Ergebnisse der Untersuchung sind in Abbildung 9 grafisch dargestellt.

---

[233] Vgl. Ripple (2017), S. 8.
[234] Vgl. Abschnitt 2.3.1.
[235] Vgl. XU (2016), S. 6; vgl. EFANOV/ROSCHIN (2018), S. 119.
[236] Vgl. HOFMANN/STREWE/BOSIA (2018), S. 39.
[237] Vgl. EFANOV/ROSCHIN (2018), S. 119.
[238] Vgl. BÖHME ET AL. (2015), S. 220 f.
[239] Vgl. SIXT (2017), S. 36.
[240] Vgl. BÖHME ET AL. (2015), S. 219 f.
[241] Vgl. MEIKLEJOHN ET AL. (2013), S. 135.

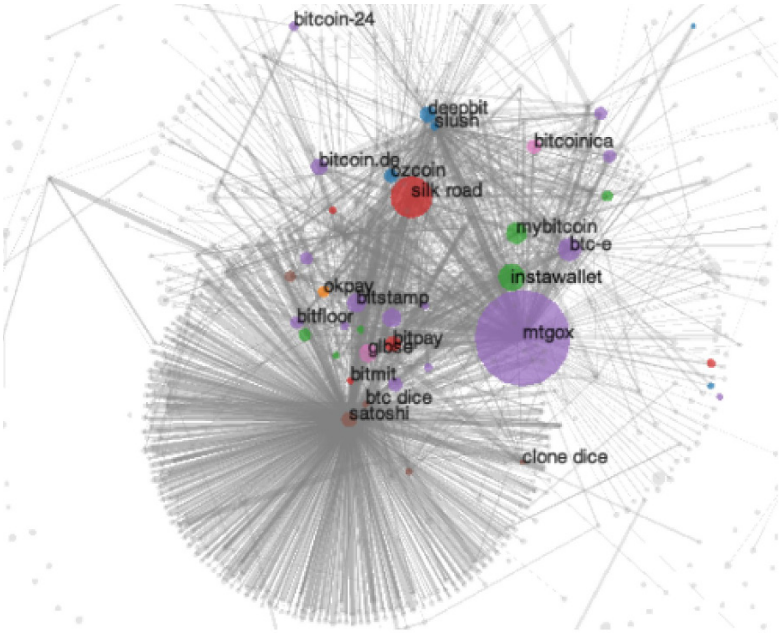


Abbildung 9: Grafische Darstellung der Zentralisierung des Bitcoin-Netzwerkes[242]

Die obige Abbildung zeigt Transaktionen zwischen unterschiedlichen Akteuren innerhalb des Bitcoin-Netzwerkes. Dabei stellt jede Verknüpfung zweier Punkte mindestens 200 Transaktionen zwischen den beiden Akteuren dar, während die Größe des Kreises das eingehende Transaktionsvolumen darstellt. Im Rahmen dieser Untersuchung konnte festgestellt werden, dass ein Großteil der Transaktionen innerhalb des Bitcoin-Netzwerkes über bestimmte Knoten, wie beispielsweise Kryptowährungsbörsen (violett) und einfache Wallet-Dienste (grün) abgewickelt werden.[243] Der hohe Grad an Zentralisierung der Bitcoin-Blockchain lässt sich zudem anhand der folgenden Beispiele verdeutlichen. Anfang 2012 wurden über 80% des gesamten Bitcoin-Handels über die Kryptobörse Mt. Gox abgewickelt. Im Zeitraum von Oktober 2014 bis März 2015 wurden sogar 95% des weltweiten Bitcoin-Transaktionsvolumens von lediglich sieben Kryptowährungsbörsen abgewickelt.[244] Wallet-Anbieter und insbesondere Kryptowährungsbörsen können somit als Intermediäre des vermeintlich dezentralen Bitcoin-Netzwerks angesehen werden.[245] Im nachfolgenden soll die Sicherheit dieser de facto Intermediäre mit denen der traditionellen Finanzintermediäre in privaten Blockchains verglichen werden.

---

[242] Quelle: Aus MEIKLEJOHN ET AL. (2013), S. 135; Republished with permission of ACM (Association for Computing Machinery) from: A fistful of bitcoins: characterizing payments among men with no names. Proceedings of the 2013 conference on Internet measurement conference, MEIKLEJOHN, S./POMAROLE, M./JORDAN, G./LEVCHENKO, K./MCCOY, D./VOELKER, G. M./SAVAGE, 2013; permission conveyed through Copyright Clearance Center, Inc.

[243] Vgl. MEIKLEJOHN ET AL. (2013), S. 135.

[244] Vgl. BÖHME ET AL. (2015), S. 220.

[245] Vgl. BÖHME ET AL. (2015), S. 219 f; vgl. BOTT/MILKAU (2016), S. 168 f.

Während Offline-Wallets bereits ein hohes inhärentes Sicherheitsrisiko haben, ist das potenzielle Risiko eines Hackerangriffs für Kunden von Online-Wallets bedeutend größer, weil diese die privaten Schlüssel zahlreicher Nutzer an einem Ort bündeln und deshalb zunehmend zu einem attraktiven Ziel für Hackerangriffe werden.[246] Die Auswirkungen eines erfolgreichen Angriffs auf die Intermediäre öffentlicher Blockchains sind verheerend. Zu Beginn des Jahres 2014 musste die bis dato größte Kryptowährungsbörse Mt. Gox infolge eines Hackerangriffs, bei dem ca. 750.000 Bitcoins der Nutzer verloren wurden, Insolvenz anmelden. Der Marktwert der Kryptotoken betrug zu diesem Zeitpunkt zwischen 220 und 370 Mio. Euro.[247] Dabei handelt es sich nicht um die einzige Insolvenz einer Kryptowährungsbörse. MOORE/CHRISTIN/SZURDI haben 80 Kryptowährungsbörsen im Zeitraum von 2010 bis 2015 untersucht und dabei festgestellt, dass innerhalb dieses Zeitraums 38 Börsen ihre Dienste wieder einstellen mussten. Zudem konnten sie bei 15 der 38 geschlossenen Börsen mindestens einen erfolgreichen Angriff auf die Sicherheitsinfrastruktur feststellen.[248]

Aufgrund dieser Sicherheitsrisiken rücken die de facto Intermediäre öffentlicher Blockchains zunehmend in den Fokus der Gesetzgebung. Die EU-Kommission sieht bspw. zukünftig die Anwendung strengerer Auflagen für die Betreiber von Kryptowährungsbörsen und Wallet-Anbietern vor. Zum einen müssten diese Dienste in jedem EU-Mitgliedsstaat lizensiert und registriert werden, in dem sie tätig werden wollen. Zum anderen müsste die Geschäftsführung dieser Dienste auf ihre persönliche und fachliche Eignung überprüft werden.[249] In den USA ist eine derartige Lizensierung für Kryptowährungsbörsen bereits verpflichtend.[250] Nach Ansicht der European Banking Authority (EBA) sind diese Dienste allerdings trotz Lizensierung weiterhin als sehr riskant einzustufen. Eine Gleichstellung von Kryptobörsen und Banken ist laut EBA nicht möglich, da für Kryptobörsen bankübliche Sicherheitsmechanismen, wie z. B. der Einlagenschutz nicht verpflichtend sind.[251]

Bei den Intermediären der untersuchten privaten Blockchains handelt es sich um Banken.[252] Diese unterliegen einem dichten Netz regulatorischer Vorgaben, wie z. B. der Mindestanforderungen an das Risikomanagement[253] oder die persönliche und fachliche Eignung der Geschäftsleitung.[254] Die Einhaltung dieser Vorschriften wird streng von unabhängigen nationalen und supranationalen Aufsichtsbehörden, wie z. B. der BaFin, der Bundesbank, der EZB und der EBA überwacht.[255] Diese Sicherheitsmaßnahmen können zwar die Zahlungsunfähigkeit einer Bank nicht vollständig ausschließen, durch Mechanismen, wie z. B. der Absicherung von Einlagen bis zu einem Betrag i. H. v. 100.000€,[256] bieten traditionelle Finanzintermediäre privater Blockchains ihren Kunden im Gegensatz zu den de facto Intermediären des öffentlichen Blockchain-Ansatzes einen gesetzlich zugesicherten Schutz. Im Hinblick auf die Sicherheit zentraler

[246] Vgl. BOIREAU (2018), S. 10.
[247] Vgl. SIXT (2017), S. 93.
[248] Vgl. MOORE/CHRISTIN/SZURDI (2016), S. 8f.
[249] Vgl. VANDEZANDE (2017), S. 350 f.
[250] Vgl. BÖHME ET AL. (2015), S. 220.
[251] Vgl. EBA (2013), S. 2.
[252] Vgl. Abschnitt 3.1.2.
[253] Vgl. BaFin (2014).
[254] Vgl. EZB (2017a), S. 10 f,
[255] Vgl. SIXT (2017), S. 124.
[256] Vgl. BaFin (2014).

Intermediäre ist der Private-Blockchain-Ansatz folglich dem Public-Blockchain-Ansatz eindeutig vorzuziehen.

3.3.3 Flexibilität bei der Auswahl des Konsensmechanismus

Die zuvor beschriebenen Unterschiede hinsichtlich Transparenz und Zugangsmodell wirken sich neben Faktoren wie dem Datenschutz und der Sicherheit der Intermediäre auch auf andere Elemente der Blockchain aus. Hierbei sind insbesondere die Auswirkungen auf die Wahl des Konsensprotokolls hervorzuheben. Da öffentliche Blockchains mit dem Ziel der Anonymität, bzw. Pseudonymität von Netzwerkteilnehmern erstellt werden, können diese bei Fehlverhalten nicht außerhalb der Blockchain-Ökosphäre belangt werden.[257] Zudem existiert kein zentraler Intermediär, welcher Vertrauen zwischen den Transaktionspartnern schaffen könnte. Daher muss in öffentlichen Blockchains zwangsläufig ein Mechanismus implementiert werden, welcher die Einigung auf eine bestimmte Transaktionshistorie ermöglicht, ohne dass die Akteure hierzu einander vertrauen müssen.[258]

Hierzu werden in den untersuchten öffentlichen Blockchains neben kryptografischen Verfahren auch spieltheoretische Mechaniken in den Prozess der Transaktionsbestätigung- und Archivierung implementiert. Um einen Transaktionsblock an die Blockchain anhängen zu können, müssen Full-Nodes ex ante einen Arbeitsnachweis in Form von aufgewendeter Rechenleistung erbringen, das sog. **Mining**.[259] Hierbei müssen die Full-Nodes zur Bestätigung von Transaktionsblöcken eine komplexe mathematische Zufallsaufgabe lösen.[260] Dieser ressourcenintensive Prozess soll betrügerisches Verhalten aus wirtschaftlicher Hinsicht unattraktiv gestalten und so einen Konsens zwischen Akteuren ermöglichen, die einander aufgrund ihrer Anonymität, bzw. Pseudonymität nicht vertrauen können.[261] Im Gegenzug für die erbrachte Rechenleistung erhalten Full-Nodes, die einen gültigen Block zur Blockchain beitragen können, eine Entlohnung in Form der Transaktionsgebühren pro validiertem Block. Zusätzlich werden mit jedem erfolgreich an die Blockkette angehängten Transaktionsblock neue Einheiten der nativen Kryptowährung geschaffen und an den Miner, der besagten Block erstellt hat, ausgegeben.[262]

Auch in privaten Blockchain-Netzwerken können Anreizsysteme für regelkonformes Verhalten implementiert werden. Hyperledger verfügt beispielsweise über einen integrierten Consensus Manager, welcher die Erstellung von Blockchain-Netzwerken mit unterschiedlichen Konsensprotokollen ermöglicht. Hiermit können auch vertrauenslose Mechanismen zur Konsensfindung gewählt werden.[263] Allerdings kann bei privaten Blockchains aufgrund der eindeutigen Identifizierbarkeit der teilnehmenden Akteure Fehlverhalten auch außerhalb des Blockchain-Ökosystems geahndet werden, indem beispielsweise strafrechtliche Maßnahmen gegen betrügerische Teilnehmer eingeleitet werden. Somit ist in Blockchains dieses Ansatzes ein vertrauensloser Konsensmechanismus nicht zwangsläufig notwendig.[264] Private Blockchains verfügen

---

[257] Vgl. PINNA/RUTTENBERG (2016), S. 11.
[258] Vgl. XU (2016), S. 2 f.
[259] Vgl. HILEMAN/RAUCHS (2017), S. 21; vgl. PINNA/RUTTENBERG (2016), S. 11 f.
[260] Vgl. Abschnitt 2.2.2.
[261] Vgl. MILKAU (2017), S. 23 f.
[262] Vgl. BÖHME ET AL. (2015), S. 218.
[263] Vgl. KIENZLER (2016), S. 114.
[264] Vgl. PINNA/RUTTENBERG (2016), S. 11.

somit über mehr Flexibilität hinsichtlich der Wahl des Konsensmechanismus. Dies ist als Stärke gegenüber dem öffentlichen Ansatz zu werten, da mit dem gewählten Konsensmechanismus eine Vielzahl von Konsequenzen verbunden sind, welche im nachfolgenden Teil der Untersuchung genauer analysiert werden.

3.4 Untersuchungsteil II: Konsensmechanismen

Sowohl Bitcoin als auch Ethereum nutzen derzeit ein Proof-of-Work-Konsensprotokoll zur Validierung der Transaktionen und zur Koordination der Details der Transaktionshistorie.[265] Einzelne Elemente dieses Konsensmechanismus sind bereits bei der Beschreibung theoretischer Grundlagen, wie z. B. der Erklärung von Hash-Funktionen erwähnt worden.[266] Allerdings wurde hierbei lediglich das von Bitcoin genutzte Standard-PoW-Protokoll beschrieben. Um spezifische Unterschiede zu Ethereums PoW-Variante namens Greedy Heaviest Observed Subtree (GHOST)[267] und den in privaten Blockchains verwendeten BFT-Konsensprotokollen[268] aufzeigen und bewerteten zu können, wird der Proof-of-Work an dieser Stelle genauer betrachtet. Der Ablauf des Proof-of-Work lässt sich in vier aufeinanderfolgende Schritte unterteilen.

1. Full-Nodes sammeln empfangene Transaktionen und bündeln diese zu einem Block. Die Menge an Transaktionen pro Block ist bei Bitcoin auf eine Obergrenze von einem Megabyte (MB) begrenzt. Je nachdem wie viele Ein- und Ausgabedaten in einer Transaktion enthalten sind, können ca. 2.000 bis 4.000 Transaktionen in einem Block zusammengefasst werden.[269] Ethereum hingegen limitiert die Blockgröße über das sog. Gas-Konzept. Für Transaktion innerhalb des Ethereum-Netzwerkes muss ein Akteur Gas mit der nativen Kryptowährung Ether kaufen. Die Höhe des Gas-Preises richtet sich nach der Komplexität der Transaktion. Jede Ethereum-Transaktion hat einen Basispreis i. H. v. 21.000 Gas. Sollte es sich jedoch um eine komplexere Transaktion, wie z. B. einen Smart Contract handeln, muss zur Ausführung zusätzliches Gas bezahlt werden.[270]
2. Ist ein Block gebildet, muss ein geeigneter Block-Hash für die darin enthaltenen Transaktionen gefunden werden. Bei Bitcoin müssen die Miner nun aufgrund des stark kollisionsresistenten Aufbaus der Hash-Funktion sukzessiv mögliche Kombinationen durchprobieren, bis sie schließlich einen geeigneten Hash-Wert gefunden haben.[271]
3. Hat ein Miner den entsprechenden Hash-Wert gefunden, wird der dazugehörige Block in die Blockchain aufgenommen, indem er im Netzwerk verteilt und von den anderen Full-Nodes gespeichert wird.[272]

---

[265] Vgl. LI ET AL. (2017), S. 3.
[266] Vgl. Abschnitt 2.2.2.
[267] Vgl. VUKOLIĆ (2016), S. 120.
[268] Vgl. VUKOLIĆ (2016), S. 116.
[269] Vgl. PLOOM (2016), S. 126.
[270] Vgl. NARAYANAN ET AL. (2016), S. 266 f.
[271] Vgl. SEITZ (2016), S. 169.
[272] Vgl. SEITZ (2016), S. 170 f; vgl. COCCO/MARCHESI (2016), S. 4.

4. Die restlichen Nodes akzeptieren das Ergebnis, sofern alle im Block enthaltenen Transaktionen valide sind, d.h. sofern die Kryptotokens nicht zuvor für eine andere Transaktion verwendet wurden und der erzeugte Block kann an die Blockchain angehängt werden.[273]

Nach Akzeptanz eines Blocks erfolgt der Proof-of-Work für den nächsten Block und beginnt somit wieder bei Schritt 1.[274] Bitcoin sieht eine zehnminütige **Blockfrequenz** zwischen der Generierung einzelner Blöcke vor.[275] Dieser zehnminütige Blockzyklus ist ein integraler Bestandteil der Proof-of-Work-Mechanik von Bitcoin und wird durch die konstante Anpassung des Schwierigkeitsgrades der Hash-Ermittlung an die Gesamtrechenleistung des Netzwerks gesteuert.[276] Je nachdem wie hoch der Schwierigkeitsgrad festgelegt wurde, muss der gewünschte Hash mit einer bestimmten Anzahl an Nullen beginnen.[277] Die Anpassung auf ein konstantes Intervall zwischen der Generierung neuer Blöcke soll verhindern, dass zu viele Blöcke in zu kurzer Zeit generiert werden und hierdurch die einzelnen Nodes mit einer Datenflut konfrontiert werden, welche diese nicht mehr verarbeiten können.[278]

Das Ethereum-Protokoll hingegen hat bedeutend kürzere Blockintervalle. Diese betragen im Durchschnitt zwischen 12 und 15 Sekunden. Somit lassen sich im Ethereum-Netzwerk mehr Transaktionen durchführen, allerdings konnten in einigen Studien infolge der verkürzten Blockzyklen auch Koordinationsprobleme zwischen den Full-Nodes festgestellt werden.[279] Diese und weitere Unterschiede werden in den einzelnen Abschnitten dieses Untersuchungsteils genauer betrachtet. Zuvor soll jedoch das BFT-Konsensprotokoll erklärt werden, dessen Varianten aktuell von privaten Blockchains, insbesondere im Finanzwesen präferiert werden.[280]

Beim BFT-Konsensprotokoll handelt es sich um ein teilweise vertrauensbasiertes Konsensprotokoll, bei dem die Full-Nodes einander zwar nicht trauen, aber einander kennen müssen.[281] Die untersuchten privaten Blockchains Ripple und Hyperledger nutzen beide unterschiedliche Varianten des BFT.[282] Grundsätzlich erfolgt die Konsensfindung bei BFT-Protokollen dadurch, dass eine vordefinierte Mindestanzahl an Netzwerkknoten einer bestimmten Transaktionshistorie zustimmt.[283] Bezüglich der genauen Ermittlung dieser Mindestanzahl unterscheiden sich der **Ripple Protocol Consensus Algorithm (RPCA)** und der von Hyperledger verwendete **Practical Byzantine Fault Tolerant (PBFT)** deutlich voneinander. Beim PBFT ist die Anzahl der Full-Nodes an die mögliche Anzahl betrügerischer oder fehlerhafter Netzwerkknoten gebunden. Zur Ermittlung der Anzahl wird folgende Formel verwendet: $n = 3f + 1$, wobei n für die Gesamtanzahl an Nodes und f für die maximale Anzahl an betrügerischer Nodes steht.[284] Beim RPCA hingegen wird zur Konsensfindung stets eine Teilmenge der verfügbaren Nodes

[273] Vgl. NAKAMOTO (2008), S. 3.
[274] Vgl. NAKAMOTO (2008), S. 3.
[275] Vgl. BOTT/MILKAU (2016), S. 160.
[276] Vgl. COCCO/MARCHESI (2016), S. 4 f.
[277] Vgl. SEITZ (2016), S. 169f; vgl. COCCO/MARCHESI (2016), S. 4.
[278] Vgl. SOMPLONSKY/ZOHAR (2018), S. 48.
[279] Vgl. GRAMOLI (2017), S. 5.
[280] Vgl. BALIGA (2017), S. 10; vgl. VUKOLIĆ (2016), S. 116.
[281] Vgl. SCHWARTZ/YOUNGS/BRITTO (2014), S. 3; vgl. VUKOLIĆ (2016), S. 116.
[282] Vgl. FREUND (2017), S. 70.
[283] Vgl. Bundesbank (2017a), S. 38.
[284] Vgl. CASTRO/LISKOV (1999), S. 2 f.

bestimmt. Die Anzahl und Zusammensetzung dieser Teilmenge wird durch eine Liste an vertrauenswürdigen Nodes, die sog. Unique Node List (UNL) bestimmt, wobei jeder Akteur eine eigene UNL erstellt.[285] Trotz dieser Unterschiede erfolgt die Konsensfindung bei beiden BFT-Varianten in drei Schritten.

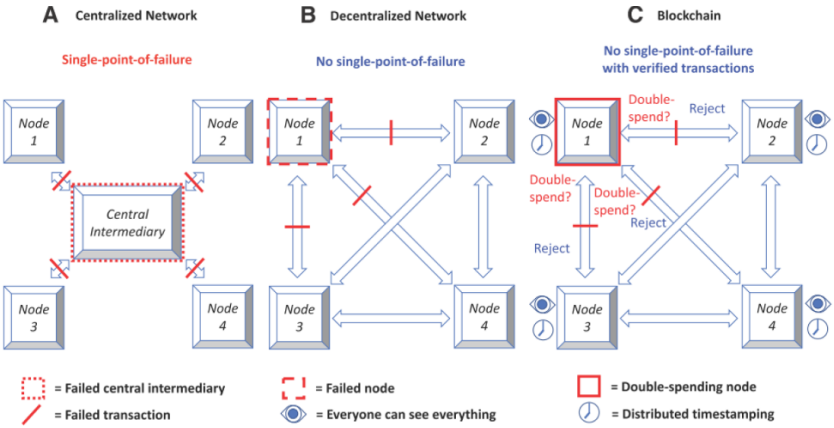
1. Full-Nodes empfangen die zu bestätigenden Transaktionen.
2. Anschließend bestätigen sie gültige Transaktionen und lehnen fehlerhafte ab. Die Ergebnisse werden von den Nodes mit dem Netzwerk kommuniziert. Hierbei ist jedoch darauf hinzuweisen, dass RPCA und PBFT unterschiedliche Schwellenwerte für die Akzeptanz von Transaktionen aufweisen. Beim PBFT müssen f+1 Antworten mit dem gleichen Ergebnis vorliegen,[286] um vom Netzwerk akzeptiert zu werden. Beim RPCA müssen zum Bestätigen von Transaktionen mindestens 80% der UNL des Transaktionsinitiators zustimmen.[287]
3. Mit der Bestätigung der Transaktionen wird der Transaktionsblock in die Blockchain aufgenommen.[288]

Der Vergleich zwischen den BFT-Varianten privater Blockchains und den PoW-Varianten öffentlicher Blockchains zeigt bereits beim Ablauf der Konsensfindung deutliche Unterschiede zwischen den beiden Ansätzen. Zur Einschätzung, ob die Unterschiede als Stärke oder Schwäche eines Ansatzes angesehen werden können, sollen in den weiteren Abschnitten dieses Untersuchungsgebietes die kritischen Erfolgsfaktoren Redundanzgrad, Leistungsfähigkeit, Settlementfinalität, Manipulationsresistenz, Full-Nodes und Einsatz der nativen Kryptowährung untersucht werden. Die jeweiligen Bewertungskriterien werden, wie bereits im ersten Untersuchungsteil zu Beginn des jeweiligen Abschnitts vorgestellt.

[285] Vgl. SCHWARTZ/YOUNGS/BRITTO (2014), S. 3.
[286] Vgl. CASTRO/LISKOV (1999), S. 2 f.
[287] Vgl. SCHWARTZ/YOUNGS/BRITTO (2014), S. 4
[288] Vgl. BALIGA (2017), S. 9 f.

3.4.1 Redundanz

Sowohl bei privaten, als auch bei öffentlichen Blockchains handelt es sich um verteilte Systeme, welche sich durch einen hohen Redundanzgrad auszeichnen. Durch einen redundanten Netzwerkaufbau vermeiden Blockchains kritische Einzelkomponenten. Dies wiederum führt zu einer Erhöhung der Widerstandsfähigkeit des Netzwerks, da selbst beim Ausfall mehrerer Komponenten kein Totalausfall des Netzwerkes droht.[289] Zur Verdeutlichung empfiehlt sich ein direkter Vergleich zwischen einem zentralisierten Netzwerk, einem simplen dezentralen Netzwerk und einer Blockchain, wie in der nachfolgenden Abbildung 10 dargestellt ist.



Source: KUO, T.-T./KIM, H.-E./OHNO-MACHADO, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017 Nov; 24(6): p 1212. By permission of © Oxford University Press

Abbildung 10: Vergleich unterschiedlicher Netzwerktypen[290]

In einem zentralisierten Netzwerk, wie dem Beispiel A in der Abbildung 10 sind sämtliche Netzwerkteilnehmer auf einen zentralen Intermediär angewiesen. Hierdurch entsteht ein sog. single-point-of-failure, da beispielsweise im Falle eines Angriffs oder einer technischen Störung keine Verbindung mehr zur zentralen Institution möglich ist. Dementsprechend sind für die Dauer des Angriffs, bzw. der Störung keine Transaktionen mehr möglich.[291]

In dezentralen Netzwerken (Beispiel B) hingegen gibt es keine kritischen Einzelkomponenten. Der Ausfall eines Teilnehmers verhindert zwar Transaktionen mit diesem Teilnehmer, allerdings ist der Rest des Netzwerks weiterhin lauffähig.[292] Der Wegfall eines Intermediäres setzt dezentrale Netzwerke jedoch dem Risiko des Double Spendings aus. Dieses wird in Blockchains, wie bereits im zweiten Kapitel der vorliegenden Arbeit erläutert, durch den Einsatz kryptografischer Verfahren eliminiert. Die chronologische Verknüpfung der einzelnen Blöcke der Transaktionshistorie unter Zuhilfenahme von Hash-Funktionen sorgen zusammen mit der

[289] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1211 f.
[290] Quelle: Aus KUO/KIM/OHNO-MACHADO (2017), S. 1212; mit freundlicher Genehmigung von © Oxford University Press.
[291] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1212.
[292] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1211 f.

öffentlichen Einsehbarkeit der Transaktionshistorie dafür, dass versuchte Double Spending Angriffe einzelner Teilnehmer zeitnah von den restlichen Netzwerkmitgliedern erkannt und abgelehnt werden können.[293] Die Vermeidung eines Single-point-of-failures ist bei Blockchains jedoch nicht nur im Hinblick auf die Kommunikation zwischen den Netzwerkteilnehmern gegeben. Auch die dezentrale Speicherung der Transaktionshistorie auf allen Full-Nodes trägt maßgeblich zur Widerstandsfähigkeit des Netzwerks bei, da sie das Risiko des Datenverlustes stark reduziert und hierdurch eine hohe Persistenz der Daten ermöglicht.[294] Dementsprechend kann ein hoher Redundanzgrad als Stärke betrachtet werden, während ein geringer Redundanzgrad als Schwäche bewertet werden kann.

Allgemein kann die redundante Infrastruktur von Blockchains, unabhängig vom gewählten Ansatz, hinsichtlich der Sicherheit des Systems als klare Stärke der Technologie identifiziert werden. Beim Vergleich des Redundanzgrades der untersuchten Blockchains lassen sich jedoch gravierende Unterschiede zwischen den beiden Blockchain-Ansätzen feststellen. Das Bitcoin-Netzwerk verfügte im Jahr 2016 über 6000 bis 6.500 Full-Nodes. Im selben Zeitraum lag die Anzahl an Full-Nodes in der ebenfalls öffentlichen Blockchain Ethereum bei 4.000 bis 5.000.[295] Eine nachträgliche Manipulation der Transaktionshistorie müsste dementsprechend nicht nur in einer zentralen Datenbank, sondern in den Aufzeichnungen aller Geräte erfolgen. Aufgrund der konstanten Überwachung des Distributed Ledgers durch alle Full-Nodes des Netzwerkes müsste diese Veränderung zudem zeitgleich erfolgen, da eine Veränderung der Transaktionshistorie auf einzelnen Netzwerkknoten schnell erkannt und durch eine Kopie des Originals ersetzt werden würde.[296]

Hierzu ist allerdings anzumerken, dass mit zunehmendem Wachstum der Transaktionshistorie auch die Anforderungen an die Speicherkapazitäten der Full-Nodes wachsen. Die Bitcoin-Blockchain ist beispielsweise inzwischen auf ca. 150 Gigabyte (GB) angewachsen.[297] Diese Datenmenge kann auf mobilen Geräten nicht mehr gespeichert werden und stellt auch für herkömmliche Privatcomputer eine Herausforderung dar. Betroffene Netzwerkteilnehmer können zwar durch den Umstieg auf eine Thin-Node-Software weiterhin Transaktionen tätigen und somit Teil des Netzwerkes bleiben. Im Hinblick auf die Widerstandsfähigkeit des Netzwerkes ist dies jedoch negativ zu bewerten, da Thin-Nodes keine Transaktionen validieren und auch nicht die vollständige Transaktionshistorie speichern. Dementsprechend führt ein Anstieg der Anzahl an Thin-Nodes zu einer Senkung der Sicherheit der Blockchain.[298]

Trotz möglicher Komplikationen infolge einer wachsenden Transaktionshistorie zeichnen sich öffentliche Blockchains derzeit durch einen deutlich höheren Redundanzgrad als ihre privaten Pendants aus. So steht den tausenden Full-Nodes der öffentlichen Blockchains eine im Juli 2017 erreichte Anzahl von 55 Full-Nodes in der privaten Blockchain Ripple gegenüber.[299] Zudem verwendet Ripple ein sog. History Sharding. Dies bedeutet, dass Ripples Validator-Nodes im

---

[293] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1212.
[294] Vgl. JENTZSCH (2016), S. 656; vgl. SÜRMELI ET AL. (2017), S. 600.
[295] Vgl. PLOOM (2016), S. 125.
[296] Vgl. XU (2016), S. 5; vgl. EZB (2016a), S. 2.
[297] Vgl. Blockchain.info (2018), Stand am 01.01.2018: 149.276 MB.
[298] Vgl. ACHENBACH/BAUMGART/RILL (2017), S. 675.
[299] Vgl. MARQUER (2017).

Gegensatz zu Full-Nodes im Bitcoin- oder Ethereum-Netzwerk nur einen Teil der Transaktionshistorie lokal auf ihrem Gerät speichern. Die Archivierung der gesamten Transaktionshistorie erfolgt im Ripple-Netzwerk auf speziellen Servern.[300] Im Hinblick auf die Widerstandsfähigkeit des Netzwerks ist der höhere Redundanzgrad öffentlicher Blockchains folglich als Stärke des öffentlichen Ansatzes gegenüber dem Privaten zu sehen. Allerdings wirkt sich der Redundanzgrad eines Netzwerks neben der Sicherheit auch auf dessen Leistungsfähigkeit aus. Dies wird im nächsten Abschnitt genauer betrachtet.

3.4.2 Leistungsfähigkeit

Die Leistungsfähigkeit ist ein wichtiges Kriterium zur Feststellung, ob einer der beiden Blockchain-Ansätze in der Lage ist, zukünftig die bisher verwendeten Altsysteme (Legacy-Systeme) abzulösen.[301] Blockchains werden besonders hinsichtlich dieses Erfolgsfaktors stark kritisiert. Allerdings wird bei dieser Kritik häufig nicht zwischen dem gewählten Blockchain-Ansatz differenziert.[302] Im Nachfolgenden soll die Leistungsfähigkeit öffentlicher und privater Blockchains untersucht werden. Diese kann gemäß VUKOLIĆ als Anzahl möglicher Transaktionen pro Zeiteinheit definiert werden.[303] Neben einer direkten Gegenüberstellung der Leistungsfähigkeit der Blockchains beider Ansätze soll durch den Vergleich mit einem Referenzwert festgestellt werden, ob öffentliche und private Blockchains dazu in der Lage wären, aktuell genutzte Verfahren zu ersetzen. Hierzu wird neben den untersuchten Blockchains auch das durchschnittliche Transaktionsvolumen im bargeldlosen Zahlungsverkehr innerhalb der EU betrachtet.

Im Bitcoin-Netzwerk sind aktuell bis zu sieben,[304] im Ethereum-Netzwerk zwischen 10 und 20 Transaktionen pro Sekunde möglich.[305] Im Vergleich dazu ermöglicht Ripple bis zu 50.000 Transaktionen pro Sekunde.[306] Erste Versuche mit der Hyperledger-Blockchain zeigen, dass in einem geschlossenen System mit 15 Full-Nodes, welche über eine entsprechend schnelle Internetanbindung verfügen, sogar bis zu 100.000 Transaktionen pro Sekunde möglich sind.[307] Es kann folglich ein inverser Zusammenhang zwischen der Anzahl validierenden Netzwerkknoten und der Leistungsfähigkeit des Netzwerkes festgestellt werden.[308] Dies wird in der nachfolgenden Abbildung 11 grafisch dargestellt.

[300] Vgl. Ripple (o. J.a).
[301] Vgl. NEYER/HUTCHISON/PORATH (2016), S. 7; vgl. HILEMAN/RAUCHS (2017), S. 19.
[302] Vgl. NEYER/HUTCHISON/PORATH (2016), S. 7.
[303] Vgl. VUKOLIĆ (2016), S. 118.
[304] Vgl. SIXT (2017), S. 96; vgl. ACHENBACH/BAUMGART/RILL (2017), S. 675.
[305] Vgl. PLOOM (2016), S. 139 f.
[306] Vgl. KAUPP/GIERA (2017), S. 253.
[307] Vgl. KIENZLER (2016), S. 120.
[308] Vgl. VUKOLIĆ (2016), S. 114.

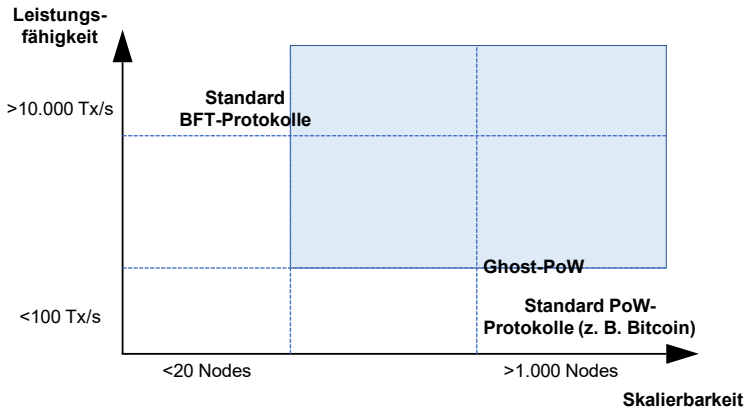


Abbildung 11: Skalierbarkeit der Konsensprotokolle PoW und BFT[309]

Während öffentliche Blockchains eine hohe Skalierbarkeit hinsichtlich der Anzahl an Full-Nodes aufweisen, zeichnen sie sich gleichzeitig durch eine stark reduzierte Leistungsfähigkeit aus. Private Blockchains hingegen sind hinsichtlich der Node-Anzahl limitiert, erzielen dafür aber eine bedeutend höhere Leistungsfähigkeit.[310] Rechnet man zuvor genannte Werte auf Tagesbasis hoch, stellt man fest, dass Bitcoin aktuell 604.800, Ethereum 1.728.000, Ripple 4.320.000.000 und Hyperledger 8.640.000.000 Transaktionen pro Tag bewältigen können. Im Vergleich dazu betrug die Gesamtanzahl an bargeldlosen Zahlungsvorgängen innerhalb der EU im Jahre 2016 laut Angaben der EZB ca. 122.000.000.000.[311] Dies entspricht einer durchschnittlichen Anzahl von 334.246.575 Transaktionen pro Tag.

Um einen direkten Vergleich der Transaktionskapazitäten öffentlicher und privater Blockchains mit dem Kapazitätsbedarf zur Verarbeitung des bargeldlosen Zahlungsverkehrs in der EU zu ermöglichen, dient die nachfolgende Tabelle 5. In dieser werden Transaktionskapazitäten pro Sekunde, Tag und Jahr jeder untersuchten Blockchain, zusammen mit dem durchschnittlichen Transaktionsvolumen des bargeldlosen Zahlungsverkehrs innerhalb der EU abgebildet.

	$\frac{Transaktionen}{Sekunde}$	$\frac{Transaktionen}{Tag}$	$\frac{Transaktionen}{Jahr}$	Eignung als Substitut für Legacy-Systeme
Legacy-Systeme	3.869	334.246.575	122.000.000.000	-
Bitcoin	7	604.800	220.752.000	Nein
Ethereum	20	1.728.000	630.720.000	Nein
Ripple	50.000	4.320.000.000	1.576.800.000.000	Ja
Hyperledger	100.000	8.640.000.000	3.153.600.000.000	Ja

Tabelle 5: Eignung der untersuchten Blockchains als Substitut für Legacy-Systeme[312]

[309] Quelle: Eigene Darstellung, in Anlehnung an VUKOLIĆ (2016), S. 114.
[310] Vgl. VUKOLIĆ (2016), S. 114.
[311] Vgl. EZB (2017b), S. 1.
[312] Quelle: Eigene Darstellung.

Vergleicht man die Leistungsfähigkeit der untersuchten Blockchains mit dem aktuellen Transaktionsvolumen innerhalb der EU, ist festzustellen, dass die Abwicklung des durchschnittlichen Transaktionsvolumens ohne Einschränkungen auf den untersuchten privaten Blockchains möglich ist. Auch Stoßzeiten, sog. Peaks, in denen laut PLOOM eine Verzehnfachung des durchschnittlichen Transaktionsvolumens auftreten kann,[313] würden bei den privaten Blockchains keine Überschreitung der Kapazitätsgrenze darstellen. Öffentliche Blockchains hingegen stoßen bereits bei einem Bruchteil des durchschnittlichen Transaktionsvolumens an die Grenzen ihrer Leistungsfähigkeit. So lassen sich mithilfe von Bitcoin ca. 0,18% und mit Ethereum ca. 0,52% des durchschnittlichen bargeldlosen Zahlungsverkehrs innerhalb der EU rechtzeitig verarbeiten. Berücksichtigt man zudem, dass sich die Summe an Zahlungsvorgängen innerhalb der EU in den vergangenen beiden Jahren um jeweils 8,5% zum Vorjahr erhöht hat,[314] sowie das mögliche Auftreten von Peaks, müssen öffentliche Blockchains ihre Performanz um ein Vielfaches steigern, damit sie als Substitut für Legacy-Systeme in Betracht gezogen werden können.

Die **geringe Transaktionskapazität öffentlicher Blockchains** ist bereits frühzeitig als Problem erkannt worden und wird seitdem in der Entwicklergemeinschaft ausgiebig diskutiert.[315] Zur Lösung wurden zwei Möglichkeiten vorgeschlagen. Einerseits könnte die **Blockgröße** erhöht werden, damit mehr Transaktionen innerhalb eines Blockes gesammelt werden können. Andererseits wäre auch ein kürzeres **Blockintervall** möglich.[316] Beide Lösungsmöglichkeiten schaffen allerdings neue Probleme. Dies sei exemplarisch am Beispiel der Bitcoin-Blockchain verdeutlicht. Eine Erhöhung der Blockgröße von aktuell einem Megabyte (MB) auf 100 MB, würde zu einer Steigerung der Leistungsfähigkeit von aktuell 7 auf maximal 700 mögliche Transaktionen pro Sekunde führen. Mit dem gestiegenen Datenvolumen steigt allerdings ggf. auch die Zeit, die ein Full-Node zum Herunterladen der aktuellen Transaktionshistorie braucht um das Hundertfache. Dies wiederum kann zu Koordinationsproblemen zwischen den einzelnen Full-Nodes führen und somit den Konsens auf eine bestimmte Transaktionshistorie erschweren.[317] Selbiges gilt auch für eine Verkürzung des Blockintervalls, da durch den verkürzten Zeitabstand unter Umständen nicht alle Nodes rechtzeitig die aktuelle Version der Blockchain auf ihrem Gerät speichern und verarbeiten konnten.[318] Allerdings ist hierbei darauf hinzuweisen, dass Ethereums PoW-Protokoll sich besser an kürzere Blockintervalle und gestiegene Blockgrößen anpasst. Diese Ergebnisse sind jedoch rein theoretisch. Ein entsprechender Stresstest mit empirisch belegten Ergebnissen ist noch nicht erfolgt.[319]

Zudem ist anzumerken, dass selbst die zuvor beschriebene Erhöhung der Blockgröße um den Faktor 100 die Transaktionskapazität von Bitcoin und Ethereum lediglich auf 700, bzw. 2000 Transaktionen pro Sekunde erhöhen würde. Hierdurch wären beide Blockchains weiterhin bereits mit der Verarbeitung des durchschnittlichen Transaktionsaufkommens ohne die starke Häufung von Transaktionen während der Stoßzeiten überfordert. Daher kann die geringe Trans-

[313] Vgl. PLOOM (2016), S. 140.
[314] Vgl. EZB (2017b), S. 1; vgl. EZB (2016b), S. 1.
[315] Vgl. PLOOM (2016), S. 140.
[316] Vgl. VUKOLIĆ (2016), S. 118.
[317] Vgl. PLOOM (2016), S. 140 f.
[318] Vgl. VUKOLIĆ (2016), S. 118.
[319] Vgl. VUKOLIĆ (2016), S. 120.

aktionskapazität des PoW öffentlicher Blockchains als inhärente Schwäche dieses Ansatzes angesehen werden.[320] Die Entwicklergemeinschaft von Ethereum möchte daher zukünftig auf einen effizienteren Konsensmechanismus, den sog. Proof-of-Stake, wechseln. Allerdings existieren hierzu aktuell nur erste Konzepte, deren Leistungsfähigkeit bislang nicht bewiesen wurde.[321]

Abschließend kann dementsprechend die geringe Leistungsfähigkeit öffentlicher Blockchains als Schwäche dieses Ansatzes bewertet werden. Zudem zeigt der Vergleich mit dem aktuellen Transaktionsaufkommen im bargeldlosen Zahlungsverkehr innerhalb der EU, dass der PoW-Konsensmechanismus öffentlicher Blockchains derzeit ein unüberwindbares Hindernis für den Einsatz dieser DLT-Varianten zur Ablösung der aktuell genutzten Systeme darstellt. Private Blockchains hingegen können innerhalb der gleichen Zeit bedeutend mehr Transaktionen abwickeln, als aktuell gefordert. Dies ist folglich als Stärke des privaten Blockchain-Ansatzes zu sehen.

3.4.3 Settlement

Der Konsensmechanismus einer Blockchain wirkt sich neben Faktoren wie dem Redundanzgrad und der Leistungsfähigkeit auch auf die Finalität des Settlements aus. Diese ist ein wichtiges Kriterium, denn gemäß der Bundesbank erfordern Finanztransaktionen: „*eine rechtlich und faktisch klar definierte Finalität, also einen bestimmbaren Zeitpunkt, ab dem eine Transaktion als gültig angesehen werden kann.*“[322] Ist diese nicht gegeben, besteht für den Zahlungsempfänger ein hohes Risiko, da der Transaktionsinitiator zwischenzeitlich zahlungsunfähig werden und somit die vereinbarte Zahlung nicht mehr leisten könnte.[323] Während in einem zentralisierten System Intermediäre wie z. B. Zentralbanken das Settlement gewährleisten und hierdurch das Risiko für den Zahlungsempfänger reduzieren,[324] unterliegt das Settlement in Blockchains den Eigenschaften und Besonderheiten des Konsensmechanismus.[325] Dieser wirkt sich neben der Finalität des Settlements auch auf die hierzu benötigte Zeit aus.[326] Da die DLT Sofortzahlungen, sog. Instant Payments, ermöglichen soll, müssen die Blockchains in der Lage sein Zahlungen innerhalb von 10 Sekunden abwickeln zu können.[327] Im Nachfolgenden soll untersucht werden, wie das Settlement in öffentlichen und privaten Blockchains erfolgt. Hierbei soll festgestellt werden, inwiefern die Blockchain-Ansätze die Anforderungen hinsichtlich Finalität und dazu benötigter Zeit erfüllen.

Öffentliche Blockchains sind P2P-Netzwerke, deren tausende Full-Nodes über den gesamten Globus verteilt sein können.[328] Hierdurch kann es zu Verzögerungen bei der Datenübertragung kommen, was dazu führt, dass verschiedene Nodes zum Teil unterschiedliche Transaktionen

[320] Vgl. VUKOLIĆ (2016), S. 118.
[321] Vgl. NEYER/GEVA (2017), S. 222.
[322] Zitat: Bundesbank (2017a), S. 43.
[323] Vgl. NEYER/GEVA (2017), S. 221.
[324] Vgl. RAMBURE/NACAMULI (2008), S. 4.
[325] Vgl. BOTT/MILKAU (2016), S. 160 f.
[326] Vgl. VUKOLIĆ (2016), S. 116f.
[327] Vgl. KAUPP/GIERA (2017), S. 253.
[328] Vgl. GENCER ET AL. (2018), S. 3.

erhalten, bestätigen und zu Blöcken bündeln.[329] Aufgrund der widersprüchlichen Informationen kann es zu einer Gabelung der Blockchain, einem sog. **Fork** kommen, da temporär zwei oder mehr „gültige“ Versionen der Transaktionshistorie vorhanden sind.[330] Bitcoin löst dieses Problem kurzfristig, indem die Miner den Block, den sie zuerst erhalten haben, als Ausgangspunkt zur Erstellung eines neuen Blockes nutzen, gleichzeitig jedoch auch den bzw. die anderen Blöcke speichern. Langfristig wird allerdings stets die längste Version der Blockchain akzeptiert.[331] Dieses Prinzip wird in der Abbildung 12 grafisch dargestellt.

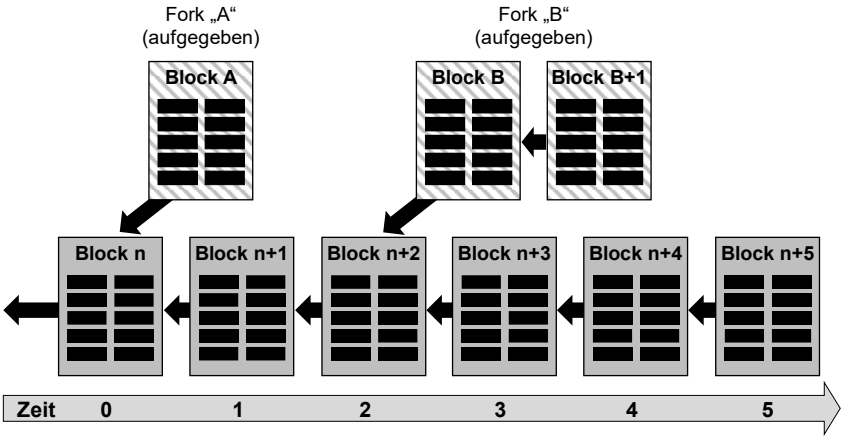


Abbildung 12: Auswahl der gültigen Transaktionshistorie im Bitcoin-Netzwerk[332]

Das bedeutet, die schraffierten Blöcke der kürzeren Blockchain werden aufgrund der Existenz einer längeren Kette mit dunkelgrau markierten Blöcken aufgegeben. Die Transaktionen in den Blöcken der parallelen Transaktionshistorie werden hierdurch verworfen und müssen erneut bestätigt werden.[333]

Mit der Einigung auf die längste verfügbare Transaktionskette unterscheidet sich Bitcoin von Ethereum. Dessen GHOST-PoW wählt im Falle eines Forks nicht den längsten, sondern den rechenintensivsten Zweig als gültige Transaktionshistorie.[334] Zur Veranschaulichung dieser Systematik dient der direkte Vergleich beider Konsensprotokolle in der Abbildung 13, bei dem mehrere Gabelungen der Transaktionshistorie abgebildet sind. In diesem Beispiel würde Bitcoin die längste Kette (schwarz) als gültige Kette wählen, während das Ethereum-Protokoll hingegen die rechenintensivste Kette (grau) als gültige Transaktionshistorie auswählen würde.[335]

---

[329] Vgl. EFANOV/ROSCHIN (2018) S. 119; vgl. XU (2016), S. 4 f.
[330] Vgl. BOTT/MILKAU (2017), S. 154.
[331] Vgl. BOTT/MILKAU (2017), S. 154.
[332] Quelle: Eigene Darstellung, in Anlehnung an SOMPLONSKY/ZOHAR (2018), S. 49.
[333] Vgl. BOTT/MILKAU (2017), S. 154.
[334] Vgl. GRAMOLI (2017), S. 5.
[335] Vgl. GRAMOLI (2017), S. 5.

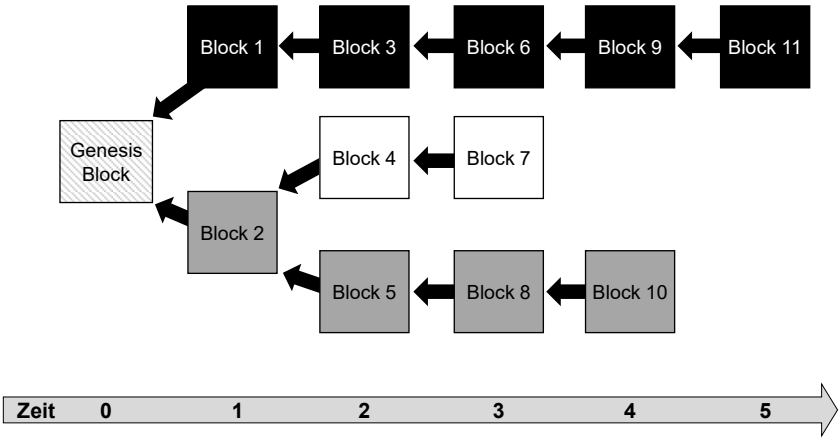


Abbildung 13: Vergleich der Konsensprotokolle von Bitcoin und Ethereum[336]

Die Aufnahme einer Transaktion in einen Block stellt bei öffentlichen Blockchains folglich kein finales Settlement dar. Vielmehr ist dies lediglich als Grundlage für ein zunehmend wahrscheinlicheres Settlement anzusehen, da wie zuvor beschrieben stets die Möglichkeit einer längeren bzw. rechenintensiveren Kette besteht. Ein finales Settlement findet in öffentlichen Blockchains dementsprechend niemals statt.[337] Stattdessen wird die Wahrscheinlichkeit, dass das Settlement als final angesehen werden kann, durch die Länge der Blockchain erhöht.[338] Als allgemeiner Richtwert für ein wahrscheinliches Settlement hat sich bei Bitcoin ein Zeitfenster von 60 Minuten, bzw. fünf auf den spezifischen Transaktionsblock folgenden Blöcken etabliert.[339] Bei Ethereum hingegen beträgt die Zeit für ein wahrscheinliches Settlement 6 Minuten, bzw. 30 auf den betrachteten Block folgende Transaktionsblöcke.[340] Es ist jedoch anzumerken, dass der Richtwert für Ethereum sich auf die Aussage einer Kryptowährungsbörse bezieht. Anders als bei Bitcoin konnte im Rahmen der Literaturrecherche kein wissenschaftlich belegtes Zeitfenster für ein höchst wahrscheinliches Settlement gefunden werden.

In den BFT-Varianten privater Blockchains bündeln die Full-Nodes hingegen nicht asynchron voneinander Transaktionen zu Blöcken und versuchen diese an die Kette anzuhängen. Stattdessen entscheiden die Full-Nodes per Mehrheitsvotum, ob individuelle Transaktionen gültig sind und zum aktuellen Transaktionsblock hinzugefügt werden können.[341] Im Ripple Netzwerk sind hierzu zwischen 3 und 6 Sekunden notwendig.[342] Die Zeit zwischen Transaktionsinitiierung und Aufnahme in die Blockchain liegt bei Hyperledger laut einer gemeinsamen Studie der EZB

[336] Quelle: Eigene Darstellung, in Anlehnung an GRAMOLI (2017), S. 5.
[337] Vgl. VUKOLIĆ (2016), S. 116 f.
[338] Vgl. BOTT/MILKAU (2017), S. 154; vgl. VUKOLIĆ (2016), S. 117.
[339] Vgl. BOTT/MILKAU (2016), S. 159.
[340] Vgl. Kraken (o. J.).
[341] Vgl. Hyperledger (2017), S. 4.
[342] Vgl. ROSNER/KANG (2016), S. 661.

und Bank of Japan zwischen 0,6 und 1,6 Sekunden.[343] Anders als bei den zuvor beschriebenen öffentlichen Blockchains gilt eine Transaktion in den BFT-Varianten privater Blockchains als bestätigt und damit nicht mehr umkehrbar.[344] Zusammenfassend kann folglich festgestellt werden, dass die privaten Blockchains sowohl die Finalitätsanforderung, als auch die Zeitanforderungen für Instant Payments erfüllen. Öffentliche Blockchains hingegen können keine Settlementfinalität bieten. Zudem zeichnen sie sich durch signifikant längere Bestätigungszeiten aus. Hierdurch wäre auch bei einer Vernachlässigung der Finalitätsanforderung der Private-Blockchain-Ansatz eindeutig vorzuziehen. Die Settlementfinalität hat auch Auswirkungen auf die Manipulationsresistenz der Transaktionshistorie. Allerdings sind dabei weitere wichtige Aspekte zu berücksichtigen, dementsprechend wird dieser Faktor im nächsten Untersuchungsabschnitt gesondert betrachtet.

3.4.4 Manipulationsresistenz des Konsensmechanismus

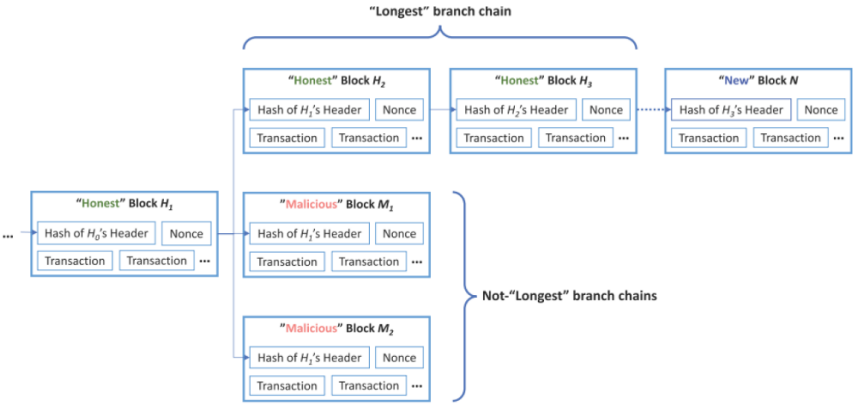
In Diskussionen bezüglich der Vorteile der DLT wird häufig auf die Fälschungssicherheit der Daten innerhalb der Blockchain verwiesen.[345] Im ersten Abschnitt dieses Untersuchungsgebietes wurde bereits festgestellt, dass der redundante Aufbau öffentlicher und privater Blockchains die Manipulation von Transaktionsdaten auf einzelnen Geräten signifikant erschwert, da derartige Veränderungen im Netzwerk sofort erkannt und durch die ständige netzwerkweite Aktualisierung der Transaktionsdaten wieder entfernt werden.[346] Dabei wurde jedoch nicht die Möglichkeit einer Manipulation des Konsensfindungsprozesses an sich berücksichtigt. Diese ist sowohl beim öffentlichen, als auch beim privaten Blockchain-Ansatz gegeben. Bezüglich des Grades der Manipulationsresistenz weisen die untersuchten Blockchains zum Teil deutliche Unterschiede auf. Dies soll im weiteren Verlauf dieses Abschnitts genauer betrachtet werden.

Die Manipulationsresistenz öffentlicher Blockchains basiert auf zwei Komponenten, dem Schwierigkeitsgrad des Block-Hashes und einem ökonomischen Anreizsystem. Erstgenannte Komponente zwingt jede Full-Node, die am Konsensfindungsprozess mitwirken möchte, dazu ex ante erhebliche Ressourcen in Form von Rechenleistung aufzuwenden.[347] Die zweitgenannte Komponente hingegen entlohnt Full-Nodes für diesen Aufwand, da diese für das Anhängen eines gültigen Blocks an die Blockkette eine gewisse Anzahl an neu geschaffenen Kryptotokens erhalten.[348] Laut FREUND ist dieses ökonomische Sicherheitsmodell die wesentliche Stärke des PoW, da es Full-Nodes in einen direkten Wettbewerb zueinander setzt. Ausgehend von der Annahme, dass Full-Nodes stets den eigenen Profit maximieren möchten, werden sie kontinuierlich die eigene Rechenleistung steigern um einen Vorteil gegenüber den anderen Netzwerkknoten zu erzielen. Hierdurch wird die Gesamtrechenleistung des Netzwerks gesteigert, wodurch wiederum der Schwierigkeitsgrad des Block-Hashes und somit die Sicherheit steigt.[349]

---

[343] Vgl. EZB/BOJ (2017), S. 6.
[344] Vgl. VUKOLIĆ (2016), S. 116 f.
[345] Vgl. BÖHME/PESCH (2017), S. 475 f; vgl. BOTT/MILKAU (2017), S. 154; vgl. SIXT (2017), S. 38.
[346] Vgl. XU (2016), S. 5; vgl. EZB (2016a), S. 2.
[347] Vgl. PINNA/RUTTENBERG (2016), S. 11 f.
[348] Vgl. BÖHME ET AL. (2015), S. 218.
[349] Vgl. FREUND (2017), S. 69.

Theoretisch sinkt hierdurch die Betrugswahrscheinlichkeit, da einzelne Nodes bei einer Mehrheit an ehrlichen Nodes nicht in der Lage sind rechtzeitig einen manipulierten Block anzuhängen, da die Mehrheit an ehrlichen Nodes immer eine längere, bzw. rechenintensivere Kette erzeugt, welche vom Konsensprotokoll stets als gültige Version der Blockchain angesehen wird.[350] Dies ist in der nachfolgenden Abbildung 14 grafisch dargestellt.



Source: KUO, T.-T./KIM, H.-E./OHNO-MACHADO, L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017 Nov; 24(6): p 1214. By permission of © Oxford University Press

Abbildung 14: Blockentwicklung bei einer mehrheitlich ehrlichen PoW-Blockchain[351]

Folglich ist es bei einer Mehrheit an ehrlichen Teilnehmern für alle Full-Nodes ertragreicher ehrlich zu bleiben, da ein Betrugsversuch zu ressourcenintensiv wäre und somit im Hinblick auf die eigene Profitmaximierung nicht sinnvoll ist.[352] PINNA/RUTTENBERG hingegen sehen in diesem ökonomischen Sicherheitsmodell die wesentliche Schwäche des PoW. So ist bereits mit einer einmaligen Investition eine vollständige Umgehung dieser Sicherheitsmechanik möglich.[353] In diesem Fall müsste ein Angreifer mindestens 51% der Gesamtrechenleistung des Netzwerkes erwerben, weshalb dieses Angriffsszenario als **51%-Attacke** bezeichnet wird. Kann ein Angreifer diesen Wert erzielen, kann er stets die längste Kette erzeugen[354] und dominiert somit vollständig den Prozess der Konsensfindung.[355]

Hat ein Angreifer die Dominanz über eine öffentliche Blockchain erlangt, kann dieser zahlreiche Manipulationen durchführen. Aufgrund der fehlenden Settlementfinalität,[356] kann er z. B. bereits getätigte Transaktionen umkehren und so die eigenen Kryptotokens mehrfach ausgeben

[350] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1214.
[351] Quelle: Aus KUO/KIM/OHNO-MACHADO (2017), S. 1214; mit freundlicher Genehmigung von © Oxford University Press. All rights reserved.
[352] Vgl. MILKAU (2017), S. 24.
[353] Vgl. PINNA/RUTTENBERG (2016), S. 12.
[354] Vgl. KUO/KIM/OHNO-MACHADO (2017), S. 1217.
[355] Vgl. XU (2016), S. 5.
[356] Vgl. Abschnitt 3.4.3.

(Double Spending) oder die Kryptotokens anderer Teilnehmer stehlen.[357] Zudem kann er bestimmte Transaktionen von der Aufnahme in die Blockchain ausschließen.[358] Obwohl bislang keine 51%-Attacke auf die Bitcoin- oder Ethereum-Blockchain erfolgt ist, besteht aufgrund eines zunehmenden Konzentrationsprozesses der Full-Nodes in PoW-basierten Blockchains ein signifikantes Sicherheitsrisiko.[359] Dieses wird unter Berücksichtigung der Erkenntnisse einer Untersuchung von EYAL/SIRER noch verstärkt. Durch Simulationen konnten sie nachweisen, dass in PoW-Blockchains eine effektive Manipulation der Transaktionshistorie bereits mit einem Anteil von 25% der Gesamtrechenleistung möglich ist.[360]

Für eine ähnliche Manipulation müsste bei Hyperledger die Kontrolle über ca. ein Drittel der Full-Nodes erlangt werden, da der PBFT immer einen sicheren Konsens erzeugen kann, sofern die Anzahl an manipulativen Nodes unterhalb des Wertes von $\frac{n-1}{3}$ liegt.[361] Bei Ripple hingegen müssen Transaktionen einen Mindestwert von 80% Zustimmung durch die Mitglieder der UNL erhalten. Folglich können Transaktionen bereits dann blockiert werden, wenn ein Angreifer mehr als 20 % der UNL kontrolliert. Allerdings müsste zum Einfügen fehlerhafter Transaktionen der Anteil an kontrollierten Full-Nodes auf 80% einer UNL ansteigen.[362] Aufgrund des geringen Redundanzgrades privater Blockchains müsste ein Angreifer lediglich die Kontrolle über ein paar einzelne Nodes erlangen, um eine Manipulation der Blockchain durchführen zu können.[363] Dabei muss jedoch berücksichtigt werden, dass private Blockchains auch innerhalb von privaten Netzwerken operieren können, welche zum Schutz vor externen Zugriffen spezielle Sicherheitssysteme, sog. Firewalls, einsetzen können.[364] Zudem ist die Settlementfinalität privater Blockchains in diesem Kontext als Stärke anzusehen, da hierdurch keine Gefahr von Rückabwicklungen spezifischer Transaktionen besteht. Zusammenfassend kann also festgestellt werden, dass private Blockchains sich aufgrund ihres Aufbaus und ihrer Konsensmechanismen wesentlich resistenter gegen Manipulationsversuche erweisen als ihre öffentlichen Konterparts. Dies ist als Stärke des privaten, bzw. als Schwäche des öffentlichen Blockchain-Ansatzes zu werten.

3.4.5 Full-Nodes: Miner vs. Validator

Die stark divergierenden Anforderungen der Konsensmechanismen öffentlicher und privater Blockchains resultieren in deutlichen Unterschieden zwischen den als Miner[365] bezeichneten Full-Nodes öffentlicher Blockchains und den Validators[366] des privaten Ansatzes. In diesem Untersuchungsabschnitt soll festgestellt werden, inwieweit diese Unterschiede einen Einfluss auf die Sicherheit des Netzwerks und die Höhe der Transaktionskosten haben. Dabei wird ein

[357] Vgl. XU (2016), S. 5.
[358] Vgl. LI ET AL. (2017), S. 7f.
[359] Dies wird im Abschnitt 3.4.5 ausführlich beschrieben.
[360] Vgl. EYAL/SIRER (2014), S. 446 f.
[361] Vgl. CASTRO/LISKOV (1999), S. 2; vgl. Abschnitt 3.4.
[362] Vgl. SCHWARTZ/YOUNGS/BRITTO (2014), S. 4.
[363] Vgl. FREUND (2017), S. 70 f.
[364] Vgl. FREUND (2017), S. 72.
[365] Vgl. XU (2016), S. 2.
[366] Vgl. ROSNER/KANG (2016), S. 677.

positiver Einfluss auf diese beiden Kriterien als Stärke, ein negativer Einfluss hingegen als Schwäche eines Ansatzes betrachtet.

Da der Schwierigkeitsgrad des PoW in direkter Verbindung zur kumulierten Rechenleistung des Netzwerks steht, muss ein Miner im Fall einer Steigerung der Gesamtrechenleistung des Netzwerks die eigene Rechenleistung steigern, um weiterhin effektiv am Mining partizipieren zu können.[367] Dies führte zu einem regelrechten **Wettrüsten der Miner**, welches an dieser Stelle genauer betrachtet wird.

Im Bitcoin-Arbeitspapier schlug NAKAMOTO zur Berechnung des Block-Hashes den Einsatz von herkömmlichen Zentralprozessoren (CPUs)[368] vor. Hierdurch hat jeder Miner ein Stimmgewicht, das der Anzahl bzw. Rechenleistung seiner CPUs entspricht.[369] In den ersten Jahren des Bitcoin-Minings wurden auch hauptsächlich CPUs zur Durchführung des PoW verwendet. Diese wurden jedoch sukzessiv durch leistungsfähigere Grafikprozessoren (GPUs)[370] ersetzt, welche mathematische Aufgaben bedeutend schneller lösen können als CPUs. Doch auch diese Hardware wurde mit der steigenden Rechenleistung des Gesamtnetzwerkes durch anwendungsspezifische integrierte Stromkreise (ASICs)[371] ersetzt.[372]

Gegenüber Standardschaltkreisen wie CPUs und GPUs bieten ASICs eine höhere Zuverlässigkeit, geringere Stromkosten und eine höhere Verarbeitungsgeschwindigkeit.[373] Spitzenmodelle aktueller ASICs ermitteln den Block-Hash 100 Millionenfach schneller als die 2009 verwendeten CPUs.[374] Dementsprechend führte die Etablierung von ASICs als Standard für Mining-Hardware zu einem starken Anstieg an Gesamtrechenleistung des Bitcoin-Netzwerkes.[375] Zur Verdeutlichung dient die Abbildung 15, in der die Entwicklung der Rechenleistung in Billionen Hash-Operationen (Terrahashes) pro Sekunde im Zeitraum vom 03.01.2009 bis 20.04.2018 grafisch dargestellt wird.

[367] Vgl. COCCO/MARCHESI (2016), S. 4 f.
[368] Engl. Central processing unit (CPU).
[369] Vgl. NAKAMOTO (2008), S. 3.
[370] Engl. Graphics processing unit (GPU).
[371] Engl. Application-specific integrated circuit (ASIC).
[372] Vgl. BRADBURY (2013), S. 6 f.
[373] Vgl. HERRMANN/MÜLLER (2004), S. 28-30.
[374] Vgl. FAIRLEY (2017), S. 58.
[375] Vgl. COCCO/MARCHESI (2016), S. 5.

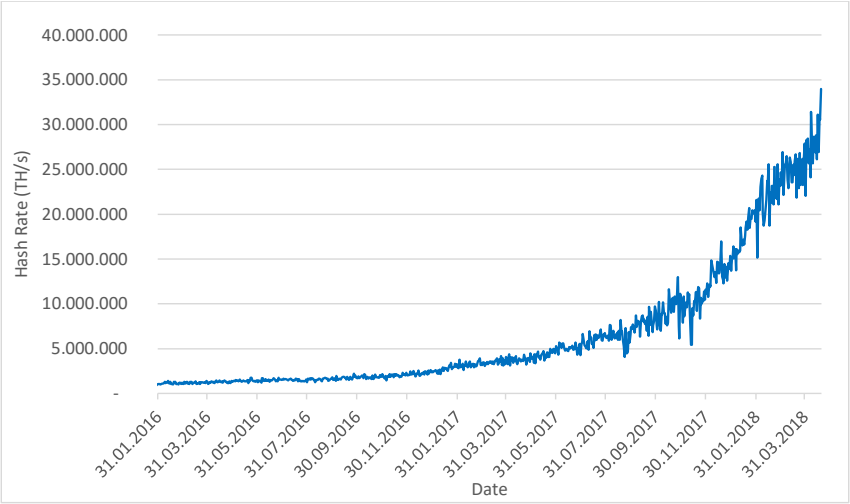


Abbildung 15: Rechenleistung des Bitcoin-Netzwerkes im Zeitraum von 31.01.2016 bis 20.04.2018[376]

Um die Leistungsfähigkeit der Bitcoin-Miner besser einschätzen zu können empfiehlt sich zudem folgender Vergleich. Laut SEITZ übertraf die kumulierte Rechenleistung aller Bitcoin-Miner zum Ende des Jahres 2015 die der 500 weltweit schnellsten Supercomputer um den Faktor 11.000.[377]

Das Hardware-Wettrüsten führte neben einer steigenden Rechenleistung auch zu einem starken Anstieg des Stromverbrauchs. Genaue Daten hinsichtlich des Stromverbrauchs öffentlicher Blockchains sind nicht verfügbar. Schätzungen gehen jedoch davon aus, dass der Stromverbrauch des Bitcoin-Netzwerkes dem kumulierten Stromverbrauch von 325.000 Haushalten entspricht.[378] Sollte die Rechenleistung des Bitcoin-Netzwerkes weiterhin derart steigen, ist zum Jahre 2020 ein Anstieg um das Zwanzigfache des aktuellen Wertes von 700 Megawatt auf insgesamt 14 Gigawatt geschätzt. Dies würde dem aktuellen Stromverbrauch des Landes Dänemark entsprechen.[379] Um die Höhe dieses Stromverbrauchs in Relation zu setzen, bietet sich ein Vergleich zwischen dem Stromverbrauch einer Bitcoin-Transaktion und einer SEPA-Überweisung an. Eine einzelne SEPA-Überweisung, ohne die Initiierung der Zahlung durch den PC oder das Smartphone des Senders, verbraucht weniger als eine Wattstunde, während der Stromverbrauch für eine äquivalente Transaktion innerhalb des Bitcoin-Netzwerkes ca. 427 Kilowattstunden beträgt. Folglich ist der Stromverbrauch im Bitcoin-Netzwerk um das 460.000-fache höher als im bisher genutzten System.[380] Gemäß BOTT/MILKAU entstehen dadurch im Bitcoin-Netzwerk „Produktionskosten" von 5 bis 10 US Dollar pro Transaktion.[381] Aufgrund des hohen

[376] Quelle: eigene Darstellung, basierend auf den Daten von Quandl (2018).
[377] Vgl. SEITZ (2016), S. 171.
[378] Vgl. FAIRLEY (2017), S. 37.
[379] Vgl. FAIRLEY (2017), S. 58.
[380] Vgl. THIELE (2018).
[381] Vgl. BOTT/MILKAU (2016), S. 158.

Stromverbrauchs wird Bitcoins PoW häufig als sinnlose Ressourcenverschwendung ohne realwirtschaftlichen Nutzen kritisiert.[382] Derartige Kritik ignoriert jedoch die Tatsache, dass eine steigende Gesamtrechenleistung die Sicherheit der Blockchain stärkt, da ein Angreifer bedeutend mehr Rechenleistung für eine erfolgreiche Manipulation der Transaktionshistorie braucht.[383]

Gleichzeitig stellt die gestiegene Rechenleistung aufgrund des ASIC-Standards jedoch auch eine Markteintrittsbarriere für Blockchains mit einem Standard-PoW dar.[384] So können Privatpersonen mit ihrer herkömmlichen Hardware nicht mehr effizient am Mining teilnehmen,[385] aber selbst durch den Erwerb geeigneter Hardware liegt die Wahrscheinlichkeit für einen einzelnen Teilnehmer einen gültigen Block zur Kette anhängen zu dürfen aktuell bei 1:600.000.[386] Da ASICs anwendungsspezifische Hardware darstellen, erfüllen sie außerhalb des jeweiligen Anwendungsgebietes, in diesem Fall dem Mining, keinen Nutzen. Dementsprechend besteht für Privatpersonen außer der Möglichkeit mit diesen Geräten am Mining zu partizipieren kein Anreiz derartige Systeme zu erwerben.[387] Darüber hinaus ist anzumerken, dass ASICs zwar an die Miningtätigkeit, aber nicht an eine spezifische Blockchain gebunden sind. Sollte beispielsweise der Preis für Bitcoin fallen und dementsprechend der Anreiz zur Validierung von Bitcoin-Transaktionen sinken, könnten Miner aufgrund fehlender Zugangsbeschränkungen problemlos ihre Rechenleistung in andere öffentliche Blockchains mit gleicher PoW-Mechanik einspeisen. Hierdurch birgt der ASIC-Standard ein hohes Fluktuationsrisiko, welches sich insbesondere auf Blockchains mit geringer Teilnehmeranzahl destabilisierend auswirken könnte.[388]

Die negativen Auswirkungen von ASICs sind bereits frühzeitig von Ethereums Entwicklergemeinschaft erkannt worden. Um ein ähnliches Wettrüsten wie im Bitcoin-Netzwerk zu vermeiden, verwendet Ethereum deshalb eine spezielle Hash-Funktion namens Ethash.[389] Ethash sieht vor, dass Miner zur Ermittlung des Block-Hash statt dem sukzessiven durchprobieren von Zufallswerten ein speicherintensives Hash-Rätsel lösen müssen. Dieses erstellt für jeden Block auf Basis des vorangegangenen Blockes einen pseudozufallsgenerierten Datensatz. Ethereum-Miner müssen anschließend einzelne Fragmente dieses Datensatzes mithilfe von Hash-Funktionen verknüpfen.[390] Aktuelle ASICs können diese speicherintensiven Vorgänge nicht effizient verarbeiten, deshalb gilt Ethash aktuell als ASIC-resistent.[391] Langfristig ist diese Wiederstandfähigkeit jedoch bedroht, da bspw. der ASIC-Produzent Bitmain noch in diesem Jahr die Markteinführung eines speziell zur Lösung von Ethash-Aufgaben ausgelegten ASICs angekündigt hat.[392]

---

[382] Vgl. SWAN (2015), S. 83.
[383] Vgl. FREUND (2017), S. 69.
[384] Vgl. SOMPLONSKY/ZOHAR (2018), S. 49 f.
[385] Vgl. GENCER ET AL. (2018), S. 9.
[386] Vgl. SOMPLONSKY/ZOHAR (2018), S. 50.
[387] Vgl. SOMPLONSKY/ZOHAR (2018), S. 50.
[388] Vgl. SOMPLONSKY/ZOHAR (2018), S. 50.
[389] Vgl. SOMPLONSKY/ZOHAR (2018), S. 50.
[390] Vgl. ZAMANOV/EROKHIN/FEDOTOV (2018), S. 395.
[391] Vgl. ZAMANOV/EROKHIN/FEDOTOV (2018), S. 395 f.
[392] Vgl. KANNENBERG (2018).

Doch auch unabhängig von anwendungsspezifischer Hardware durchläuft die Gesamtrechenleistung des Etherum-Netzwerks eine annähernd exponentielle Steigerung. Diese wird in Abbildung 16 grafisch dargestellt.

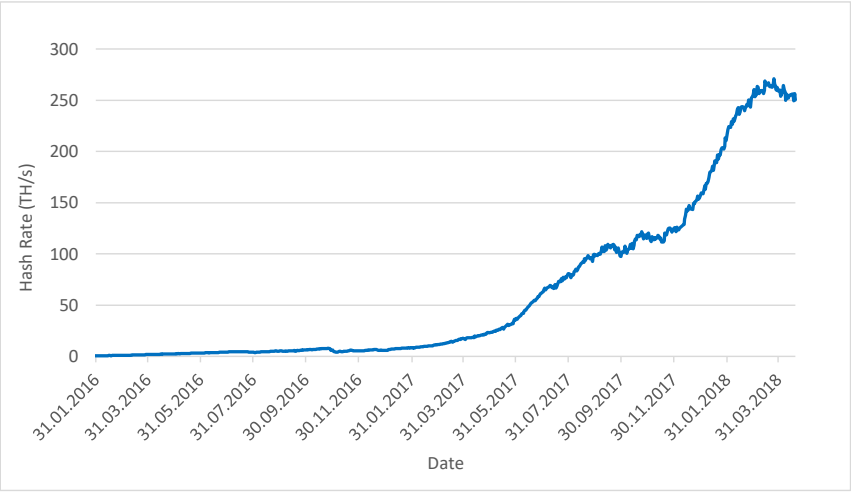


Abbildung 16: Rechenleistung des Ethereum-Netzwerkes im Zeitraum von 31.01.2016 bis 20.04.2018[393]

Mit steigender Rechenleistung steigt in PoW-Blockchains auch der Schwierigkeitsgrad. Infolge des rapide wachsenden Schwierigkeitsgrades sinken zunehmend die Erfolgschancen von isoliertem Mining und führen zu einer weiteren negativen Entwicklung in öffentlichen Blockchains, der zunehmenden Konzentration von Minern in sog. **Mining-Pools**.[394] Bei Mining Pools handelt es sich um Zusammenschlüsse von Minern, welche gemeinsam für geringfügig unterschiedliche Varianten eines Blockes Hash-Werte suchen. Für die Miner bieten diese Zusammenschlüsse zwei Vorteile. Zum einen verhindern sie die Verschwendung von Rechenkapazität durch paralleles Durchführen gleicher Berechnungen, indem unterschiedliche Variationen berechnet werden.[395] Zum anderen wird die Belohnung für das Finden eines gültigen Block-Hashes unter allen Teilnehmern eines Pools aufgeteilt.[396]

Während Mining Pools also für einzelne Miner ein Mittel zur Risikosenkung darstellen,[397] wirken sie hinsichtlich der Manipulationsresistenz des Konsensmechanismus risikosteigernd aus, da sie zur Zentralisierung des Systems beitragen.[398] Sowohl Bitcoin als auch Ethereum sind durch die zunehmende Zentralisierung durch Mining-Pools betroffen.[399] GENCER ET AL. haben Mining-Pools beider Blockchains untersucht und dabei festgestellt, dass über 90% der Gesamtrechenleistung beider Netzwerke sich bei Bitcoin auf 16 und bei Ethereum auf lediglich 11

[393] Quelle: eigene Darstellung, basierend auf den Daten von Etherscan (2018).
[394] Vgl. BÖHME ET AL. (2015), S. 222.
[395] Vgl. SOMPLONSKY/ZOHAR (2018), S. 51.
[396] Vgl. PETRLIC/SORGE (2017), S. 84.
[397] Vgl. SOMPLONSKY/ZOHAR (2018), S. 50.
[398] Vgl. PETRLIC/SORGE (2017), S. 84.
[399] Vgl. VUKOLIĆ (2016), S. 117.

Mining-Pools verteilt.[400] In der Vergangenheit sind zudem Situationen aufgetreten, in denen ein einzelner Mining-Pool mehr als 50% der Rechenleistung des Bitcoin-Netzwerk kontrollierte.[401] Im Hinblick auf die Manipulationsresistenz und somit die Sicherheit öffentlicher Blockchains ist deren hoher Grad an Zentralisierung als schwerwiegende Schwäche zu werten.

Paradoxerweise zeigt die Untersuchung von GENCER ET AL., dass in den zentralisierten privaten Blockchains mithilfe eines teilweise vertrauensbasierten BFT-Konsensprotokoll ein höherer Grad an Dezentralität erzielt werden, als bei ihren öffentlichen und somit theoretisch dezentralen Pendants. Dies ist laut GENCER ET AL. bereits mit 20 Validator-Nodes möglich.[402] Zudem zeichnen sich die Validators privater Blockchains durch einen wesentlich geringeren Stromverbrauch aus.[403] Außerdem sind die Hardwareanforderungen zum Betrieb einer Full-Node in privaten Blockchains bedeutend geringer. Laut Angaben von Ripple kann aktuell eine Validator-Node bereits mit einem Arbeitsspeicher von 8 GB und einer Festplattenkapazität von 32 GB stabil betrieben werden.[404] Leistungsfähige Grafikkarten oder ASICs werden nicht benötigt,[405] da die Full-Nodes lediglich ein Votum zu Transaktionen abgeben.[406]

Zusammenfassend kann folglich festgestellt werden, dass die Miner öffentlicher Blockchains hohe Ausgaben für die entsprechende Hardware und die Aufrechterhaltung des Mining-Prozesses haben.[407] Aufgrund der sinkenden Erfolgschancen isolierten Minings schließen sich Miner zudem zunehmend zu Kollektiven zusammen und erhöhen so die Wahrscheinlichkeit einer 51%-Attacke. Dementsprechend verursacht die Full-Node-Infrastruktur hohe Transaktionskosten, ohne einen äquivalenten Beitrag zur Sicherheit der Blockchain zu leisten. Dies ist als Schwäche des öffentlichen Blockchain-Ansatzes zu werten, während die geringen Kosten für den Erwerb der Hardware und den laufenden Betrieb der Full-Node-Infrastruktur eine Stärke des privaten Ansatzes darstellen.

3.4.6 Kryptowährung

Grundsätzlich ist die Notwendigkeit zur Implementierung einer eigenen Kryptowährung an den Aufbau und die Zielsetzung einer Blockchain gebunden. Abhängig vom gewähltem Anwendungsbereich und Konsensmechanismus können Blockchains mit, aber auch ohne native Kryptowährung operieren.[408] Zudem kann die jeweilige Kryptowährung unterschiedliche Funktionen innerhalb des Blockchain-Ökosystems erfüllen. Sie kann als universelles Zahlungsmedium, aber auch als Mittel zur systemeigenen Entlohnung für die Full-Nodes genutzt werden.[409] Je nachdem, ob und in welchem Umfang eine Kryptowährung innerhalb einer Blockchain genutzt wird, unterscheiden sich deren Auswirkungen auf die Effizienz und Sicherheit des Systems. Im Nachfolgenden wird der Einsatz von Kryptowährungen innerhalb der privaten und öffentlichen

---

[400] Vgl. GENCER ET AL. (2018), S. 10.
[401] Vgl. BÖHME ET AL. (2015), S. 222.
[402] Vgl. GENCER ET AL. (2018), S. 11.
[403] Vgl. VUKOLIĆ (2016), S. 115.
[404] Vgl. Ripple (o. J.b).
[405] Vgl. Ripple (o. J.b).
[406] Vgl. ROSNER/KANG (2016), S. 659; vgl. BALIGA (2017), S. 10.
[407] Vgl. PINNA/RUTTENBERG (2016), S. 13.
[408] Vgl. BURGWINKEL (2016), S. 36.
[409] Vgl. BURGWINKEL (2016), 36 f.

Blockchains genauer betrachtet. Hierbei soll festgestellt werden, inwieweit die spezifische Nutzung der Kryptowährung einen positiven, bzw. negativen Beitrag zur Effizienz und Sicherheit des Netzwerks hat und somit als Stärke bzw. als Schwäche bewertet werden kann.

In beiden Blockchains des öffentlichen Ansatzes sind Kryptowährungen ein zentraler Bestandteil des Ökosystems. Sowohl Bitcoin als auch Ethereum nutzen die eigene Kryptowährung als Zahlungsmedium.[410] Hierdurch soll ein von zentralen Intermediären unabhängiges Substitut für traditionelle Währungen geschaffen werden.[411] Im Gegensatz zu den meisten traditionellen Zahlungsmitteln weist Bitcoin jedoch eine höchst volatile Wertentwicklung auf, wodurch diese Kryptowährung nach MISHKIN zwei,[412] gemäß THIELE/DIEHL sogar alle drei der in Abschnitt 2.1.2 definierten Geldfunktionen nicht erfüllt.[413] Die hohe Volatilität des Bitcoin-Kurses verhindert zum einen den Einsatz als Recheneinheit, da infolge der ständigen Kursschwankungen keine stabilen Preise in Bitcoin angegeben werden können.[414] Als Mittel zur Wertaufbewahrung eignet sich Bitcoin aufgrund der extremen Kursschwankungen ebenfalls nicht.[415]

Schließlich ist auch die Eignung von Bitcoin als Tauschmedium fraglich. Die Chance auf hohe Renditen infolge der starken Wertschwankungen verbietet laut MICHAELIS auch „die Verwendung als Tauschmittel“.[416] Die hohe Volatilität ist jedoch kein Bitcoin-spezifisches Problem. Stattdessen weisen alle Kryptowährungen vergleichbare Defizite auf.[417] Als Beleg hierfür dient die nachfolgende Abbildung 17, welche die Kursverläufe von Bitcoin, Ether und Ripple im Zeitraum von Januar 2016 bis Oktober 2017 grafisch darstellt.

[410] Vgl. BRÜHL (2017a), S. 15.
[411] Vgl. BURGWINKEL (2016), S. 36.
[412] Vgl. MISHKIN (2016), S. 102.
[413] Vgl. THIELE/DIEHL (2017), S. 6.
[414] Vgl. SIXT (2017), S. 110.
[415] Vgl. MISHKIN (2016), S. 102; vgl. MICHAELIS (2017), S. 17.
[416] Zitat: MICHAELIS (2017), S. 17.
[417] Vgl. BRÜHL (2017a), S. 15.

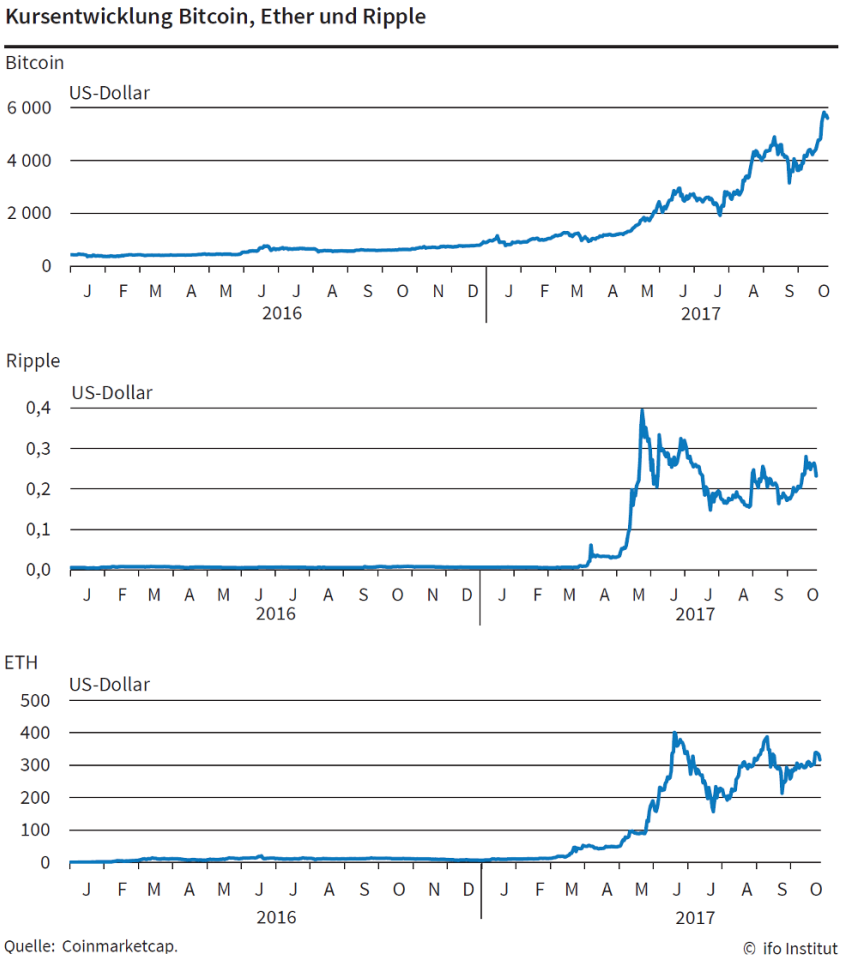


Abbildung 17: BTC-, Ripple-, und ETH- Kurs im Zeitraum von Januar 2016 bis Oktober 2017[418]

Dementsprechend zeichnen sich sowohl die Kryptowährungen der öffentlichen Blockchains Bitcoin und Ethereum, als auch die der privaten Blockchain Ripple durch eine hohe Volatilität und damit höhere Transaktionskosten aus. Im Gegensatz zu den öffentlichen Blockchains ist Ripples Kryptowährung jedoch nicht das universelle Zahlungsmedium innerhalb des Ökosystems. Stattdessen ist das Ripple-Netzwerk währungsneutral, da Zahlungen sowohl mit der nativen Kryptowährung als auch mit traditionellen Währungen wie z. B. Euro und US Dollar möglich sind.[419] Die native Kryptowährung kann somit als komplementäre Brückenwährung

[418] Quelle: Aus BRÜHL (2017a), S. 15; mit freundlicher Genehmigung von © ifo Institut.
[419] Vgl. SIXT (2017), S. 181.

für illiquide Fremdwährungsmärkte genutzt werden.[420] In Hyperledger hingegen ist keine native Kryptowährung vorgesehen. Stattdessen können verschiedene digitale Tokens als Repräsentanten für reale Vermögenswerte geschaffen werden.[421]

Zudem erfordern die BFT-Konsensmechanismen privater Blockchains keine Anreizmechanik unter Zuhilfenahme einer entsprechenden Kryptowährung.[422] In öffentlichen Blockchains ist dies jedoch zwangsläufig notwendig, da die Transaktionsgebühren bei öffentlichen Blockchains momentan nicht verpflichtend sind und eher Spenden als tatsächliche Gebühren darstellen. Mit dieser Spende soll nicht der der Transaktionsvorgang bezahlt werden, vielmehr soll diese die Aufnahme von Transaktionen in einen Block sicherstellen, da Transaktionen ohne entsprechende Gebühr bei hohen Transaktionsaufkommen häufig von den Full-Nodes ignoriert werden.[423] Der eigentliche Anreiz zum Durchführen des PoW liegt folglich in der Ausgabe neugeschaffener Kryptotokens für das Finden eines gültigen Block-Hashes, dem sog. **block reward**.[424]

Langfristig entsteht hierdurch für öffentliche Blockchains allerdings ein Sicherheitsproblem, denn die maximale Menge an neuen Kryptotokens ist i. d. R. begrenzt.[425] Bei Bitcoin können maximal 21 Millionen Tokens geschaffen werden[426] und auch die Menge an Ether soll laut dem Schöpfer und leitendem Entwickler BUTERIN auf ca. 120 Millionen Einheiten begrenzt werden.[427] Mit der Ausgabe des letzten neu geschaffen Kryptotokens entfällt die systemseitige Subvention des PoW. Somit bleiben den Full-Nodes ab diesem Zeitpunkt nur noch die Transaktionsgebühren als Anreiz für das PoW.[428] Da jedoch bereits die Stromkosten pro Transaktion im Bitcoin-Netzwerk mehr als das Fünf- bis Zehnfache der gesamten Transaktionskosten zentralisierter Systeme darstellen,[429] müssten die Transaktionsgebühren pro Transaktion massiv ansteigen, um einen Anreiz für die hohe Rechenleistung zu schaffen. Durch derart hohe Transaktionskosten wären öffentliche Blockchains jedoch nicht mehr wettbewerbsfähig. Folglich können öffentliche Blockchains langfristig nur durch eine Senkung der Gesamtrechenleistung, bzw. dem Ausstieg mehrerer Full-Nodes aus dem Netzwerk wettbewerbsfähige Transaktionskosten erzeugen.[430] Eine Reduktion der Gesamtrechenleistung wirkt sich jedoch, wie in Abschnitt 3.4.4 festgestellt wurde, negativ auf die Manipulationsresistenz des Konsensmechanismus und somit die Sicherheit des Netzwerks aus.[431]

Zusammenfassend lässt sich feststellen, dass die Notwendigkeit zum Einsatz einer nativen Kryptowährung in öffentlichen Blockchains sich sowohl im Hinblick auf die Effizienz, als auch im Hinblick auf die Sicherheit negativ auswirkt. Dementsprechend ist dieses Blockchain-Ele-

---

[420] Vgl. BRÜHL (2017b), S. 138f; vgl. ROSNER/KANG (2016), S. 675; vgl. SIXT (2017), S. 181.
[421] Vgl. Hyperledger (2017), S. 3.
[422] Vgl. BALIGA (2017), S. 12.
[423] Vgl. KAŞKALOĞLU (2014), S. 93.
[424] Vgl. ALI ET AL. (2014), S. 278.
[425] Vgl. ALI ET AL. (2014), S. 281.
[426] Vgl. BÖHME ET AL. (2015), S. 218.
[427] Vgl. BUTERIN (2018).
[428] Vgl. ALI ET AL. (2014), S. 281.
[429] Vgl. BOTT/MILKAU (2016), S. 158.
[430] Vgl. ALI ET AL. (2014), S. 281.
[431] Vgl. ALI ET AL. (2014), S. 281; vgl. Abschnitt 3.4.4.

ment als Schwäche des Public-Blockchain-Ansatzes zu sehen. Der Einsatz einer Kryptowährung ist privaten Blockchains hingegen optional. Durch die Möglichkeit zu währungsneutralen Zahlungen bzw. zur Abbildung realer Vermögenswerte unterliegen Transaktionen in privaten Blockchains nicht den negativen Auswirkungen einer nativen Kryptowährung. Auch im Hinblick auf die Sicherheit spielt die, sofern vorhandene, native Kryptowährung keine Rolle. Der optionale Einsatz nativer Kryptowährungen kann somit als Stärke des Private-Blockchain-Ansatzes gewertet werden. Mit der Bewertung des Einsatzes der Kryptowährung innerhalb der jeweiligen Blockchains endet der zweite Teil der Analyse. Die Ergebnisse beider Analyseteile werden im nachfolgenden Abschnitt zusammengefasst.

3.5 Ergebnisse der Stärken-Schwächen-Analyse

In den vorangegangenen Untersuchungsabschnitten wurde die Merkmalsausprägung 9 kritischer Erfolgsfaktoren bei beiden Blockchain-Ansätzen untersucht. Die Ergebnisse werden in der nachfolgenden Tabelle 6 innerhalb einer Stärken-Schwächen-Matrix visualisiert.

Untersuchte Faktoren	Stärke	Keine Aussage möglich	Schwäche
Untersuchungsteil 1: Zugangs- und Transparenzmodell			
– Schutz sensibler Daten	◇		◆
– Sicherheit zentraler Intermediäre	◇		◆
– Flexibilität bei der Auswahl des Konsensmechanismus	◇		◆
Untersuchungsteil 2: Konsensmechanismen			
– Redundanz	◆		◇
– Leistungsfähigkeit	◇		◆
– Settlementfinaliät	◇		◆
– Manipulationsresistenz	◇		◆
– Full-Nodes	◇		◆
– Kryptowährung	◇		◆

◇ Private-Blockchain-Ansatz ◆ Public-Blockchain-Ansatz

Tabelle 6: Stärken-Schwächen-Matrix Private- und Public-Blockchain-Ansatz[432]

Die Ergebnisse der Untersuchung zeigen, dass in 8 von 9 untersuchten Elementen der private Ansatz gegenüber dem öffentlichen vorzuziehen ist. Öffentliche Blockchains weisen lediglich hinsichtlich des möglichen Redundanzgrades eine Stärke gegenüber dem privaten Ansatz auf. Hierbei ist allerdings zu berücksichtigen, dass der Redundanzgrad sich ausschließlich auf die Anzahl an Full-Nodes bezieht. Unter Berücksichtigung der zunehmenden Zentralisierung öffentlicher Blockchains aufgrund von Mining Pools und de facto Intermediären, wie z. B. Kryptowährungsbörsen, muss dieser Vorteil kritisch gesehen werden, da durch die Zentralisierung kritische Einzelkomponenten entstehen, welche sich negativ auf die Sicherheit des Netzwerks auswirken.[433] Bei den anderen untersuchten Erfolgsfaktoren konnten signifikante Schwächen

[432] Quelle: eigene Darstellung.
[433] Vgl. BÖHME ET AL. (2015), 219-222.

des öffentlichen Ansatzes festgestellt werden. Die vollständige Datentransparenz dieses Blockchain-Ansatzes bietet, entgegen der Behauptung durch pseudonyme öffentliche Schlüssel einen besseren Schutz sensibler Daten zu gewährleisten, keine Vorteile gegenüber den eingeschränkten Leserechten privater Blockchains. Mit dem Verzicht auf Zugangsbeschränkungen und die Feststellung der Identität der Netzwerkteilnehmer sind öffentliche Blockchains zudem dazu gezwungen vertrauenslose Konsensmechanismen, wie das Proof-of-Work zu verwenden.

Dieser weist, mit Ausnahme des höheren Redundanzgrades, gegenüber den teilweise vertrauensbasierten Konsensmechanismen der privaten Blockchains signifikante Defizite auf. Erfolgsfaktorübergreifend konnte festgestellt werden, dass die Proof-of-Work-Varianten öffentlicher Blockchains eine geringere Sicherheit und Leistungsfähigkeit als die BFT-Varianten privater Blockchains bieten. Gleichzeitig führt die Verknüpfung der Sicherheitsmechanik mit einem ökonomischen Anreizsystem zu einem aktiven Wettbewerb zwischen den Full-Nodes.[434] Dies wiederum führt zu hohen Ausgaben für wettbewerbsfähige Hardware und hohen Stromkosten. Der abstimmungsbasierte Konsensprozess privater Blockchains hingegen verlangt weder spezielle Hardware noch aufwendige Berechnungen. Hierdurch kann auf einen Anreiz in Form einer systemseitigen Subvention der Transaktionskosten mit neu geschaffenen Kryptotokens verzichtet werden. Dies ist aktuell aufgrund der hohen Volatilität von Kryptowährungen, aber im Hinblick auf die Risiken nach einem Ende der Subvention auch langfristig als Stärke des privaten Ansatzes zu werten. Diese Ergebnisse werden im nächsten Kapitel zur Beantwortung der Forschungsfrage genutzt.

[434] Vgl. FREUND (2017), S. 69; vgl. SOMPLONSKY/ZOHAR (2018), S. 49.

4 Fazit

Das Ziel der vorliegenden Masterarbeit ist eine kritische Beurteilung der Blockchain bzw. Distributed Ledger Technology anhand einer differenzierten Betrachtung des Private- und des Public-Blockchain-Ansatzes. Hierzu wurden in Kapitel 1 zwei Forschungsfragen gestellt, zu deren Beantwortung, nach einer Darstellung der theoretischen Grundlagen, eine Stärken-Schwächen-Analyse durchgeführt wurde. Im Rahmen der Analyse wurde untersucht, welche Merkmalsausprägungen beide Ansätze in neun Blockchain-spezifischen kritischen Erfolgsfaktoren aufweisen. Die Ergebnisse der Untersuchung zeigen, dass der Public-Blockchain-Ansatz in der überwiegenden Mehrheit der untersuchten Erfolgsfaktoren Schwächen gegenüber dem Private-Blockchain-Ansatz aufweist. Zusammenfassend kann der Verzicht auf Vertrauen zwischen den Netzwerkteilnehmern und die Entfernung traditioneller Finanzintermediäre als inhärente ideologische Schwäche des Public-Blockchain-Ansatzes festgestellt werden. Diese Entscheidung führt bei öffentlichen Blockchains zur Nutzung von unsicheren de facto Intermediären und vertrauenslosen Konsensmechanismen, welche sich sowohl im Hinblick auf die Sicherheit, als auch auf die Effizienz dieser Netzwerke negativ auswirken. Die erste Forschungsfrage kann also folgendermaßen beantwortet werden:

> *Der Private-Blockchain-Ansatz ist dem Public-Blockchain-Ansatz eindeutig vorzuziehen.*

Auch zur Beantwortung der zweiten Forschungsfrage konnten im Rahmen der Untersuchung Belege gefunden werden. Die begrenzte Leistungsfähigkeit des Proof-of-Work öffentlicher Blockchains ist eine unumgängliche Limitation des Konsensmechanismus. Die Betrachtung von Möglichkeiten zur Steigerung der Leistungsfähigkeit des Proof-of-Work zeigt, dass leistungssteigernde Modifikationen zu neuen Schwächen wie z. B. steigenden Koordinationsproblemen führen. Auch die fehlende Settlementfinalität in öffentlichen Blockchains erweist sich als unüberwindbares Hindernis, da diese ein zwingendes Element der Proof-of-Work-Mechanik darstellt. Zudem führen hohe Ausgaben für die kompetitive Full-Node-Infrastruktur öffentlicher Blockchains dazu, dass diese zum Ende der systemseitigen Subvention hinsichtlich der Transaktionskosten ohne eine signifikante Reduktion des Redundanzgrades nicht mehr wettbewerbsfähig sind. Die fehlende Flexibilität bei der Wahl der Konsensmechanismen verweigert öffentlichen Blockchains die Nutzung leistungsfähigerer, sicherer und günstigerer teilweise vertrauensbasierter Konsensmechanismen, wie den BFT-Varianten. Leistungsfähigere vertrauenslose Konsensmechanismen, wie z. B. der Proof-of-Stake sind derzeit in der Konzeptphase und konnten aufgrund fehlender empirischer Belege der potenziellen Vorteile im Rahmen der vorliegenden Arbeit nicht berücksichtigt werden. Somit stellt der Proof-of-Work-Konsensmechanismus in Ermangelung geeigneter Alternativen zumindest aktuell ein unüberwindbares Hindernis für eine weitreichende Implementierung von Blockchains nach öffentlichem Ansatz dar. Bezüglich der privaten Blockchains konnten keine Hinweise auf unüberwindbare Hindernisse gefunden werden. Die zweite Forschungsfrage kann dementsprechend folgendermaßen beantwortet werden:

> *Sofern der Proof-of-Work nicht durch einen effizienteren und sichereren vertrauenslosen Konsensmechanismus ersetzt werden kann, stellt dieser ein unüberwindbares Hindernis zur weitreichenden Implementierung der Distributed Ledger Technology nach dem Public-Blockchain-Ansatz dar.*

V. Rutz, *Blockchain quo vadis*, BestMasters,
https://doi.org/10.1007/978-3-658-29405-2_4

Die Ergebnisse der vorliegenden Masterarbeit bestätigen somit den aktuellen Trend zum Vorzug des Private-Blockchain-Ansatzes für Anwendungen im Finanzwesen.[435] Allerdings müssen bei der Interpretation der Ergebnisse die Limitationen der Untersuchung berücksichtigt werden. Einerseits wurden mit je zwei Blockchains pro Ansatz lediglich vier spezifische Blockchain-Plattformen untersucht. Aufgrund der begrenzten Anzahl wissenschaftlicher Untersuchungen sind bei einigen Erfolgsfaktoren außerdem nicht alle Blockchains in gleichem Detailgrad erfasst worden. Zudem konnten in Ermangelung ausreichender wissenschaftlicher Literatur oder praktischer Umsetzungen bestimmte Faktoren, wie z. B. Smart Contracts oder marktprozessbedingte Adaptionsbarrieren im Rahmen der Analyse nicht berücksichtigt werden. Diese stellen jedoch laut Ansicht einiger Autoren, wie beispielsweise MORI bis zu 80% der Schwierigkeiten bei der Implementierung der Distributed Ledger Technology dar.[436] Trotz dieser Limitationen konnte eine detaillierte Betrachtung der Stärken und Schwächen beider Ansätze vorgenommen werden. Damit bietet die vorliegende Masterarbeit neben dem eigenen Erkenntnisgewinn auch einen Ausgangspunkt für zukünftige Untersuchungen des Private- und des Public-Blockchain-Ansatzes.

[435] Vgl. PINNA/RUTTENBERG (2016), S. 32; vgl. VUKOLIĆ (2016), S. 116.
[436] Vgl. MORI (2016), S. 216.

Literaturverzeichnis

ACHENBACH, D./BAUMGART, I./RILL, J. (2017). Die Blockchain im Rampenlicht. Technologie von der Stange – oder besser nach Maß? *Datenschutz und Datensicherheit, 41. Jg.* (11). S. 673-677.

AL JAWAHERI, H./AL SABAH, M./BOSHMAF, Y./ERBAD, A. (2018). When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis. S. 1-11. Verfügbar unter https://arxiv.org/pdf/1801.07501.pdf Zugriff am 23.04.2018.

ALI, R./BARRDEAR, J./CLEWS, R./SOUTHGATE, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin, Vol. 54* (3). S. 276-286.

AULIBAUER, A. G./THIEßEN, F. (2012). Finanzintermediation und Markteffizienz. In H. J. Hockmann & F. Thießen (Hrsg.), *Investmentbanking* (3., überarb. und erw. Aufl., S. 42-79). Stuttgart: Schäffer-Poeschel.

BaFin. (2014). *Bankenaufsicht,* Bundesanstalt für Finanzdienstleistungsaufsicht. Verfügbar unter https://www.bafin.de/DE/DieBaFin/AufgabenGeschichte/Bankenaufsicht/bankenaufsicht_node.html Zugriff am 23.04.2018.

BaFin. (2017). *Blockchain-Technologie,* Bundesanstalt für Finanzdienstleistungsaufsicht. Verfügbar unter https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html Zugriff am 13.12.2017.

BALIGA, A. (2017). *Understanding Blockchain Consensus Models,* Persistent Systems. Verfügbar unter https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf Zugriff am 23.04.2018.

BAUM, H.-G./COENENBERG, A. G./GÜNTHER, T. (2007). *Strategisches Controlling* (4., überarb. Aufl.). Stuttgart: Schäffer-Poeschel.

BEA, F. X./HAAS, J. (2017). *Strategisches Management* (UTB Betriebswirtschaftslehre, Bd. 8498, 9., überarbeitete Auflage). Konstanz: UVK Verlagsgesellschaft mbH; UVK/Lucius.

BEUTELSPACHER, A./NEUMANN, H. B./SCHWARZPAUL, T. (2010). *Kryptografie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld* (2., überarbeitete Auflage). Wiesbaden: Vieweg + Teubner.

Blockchain.info. (2018). *Blockchain Size,* Blockchain. Verfügbar unter https://blockchain.info/de/charts/blocks-size Zugriff am 23.04.2018.

BÖHME, R./CHRISTIN, N./EDELMAN, B./MOORE, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives, 29* (2). S. 213-238.

BÖHME, R./PESCH, P. (2017). Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. *Datenschutz und Datensicherheit, 41* (8). S. 473-481.

BOIREAU, O. (2018). Securing the blockchain against hackers. *Network Security* (1). S. 8-11.

BOLESCH, L./MITSCHELE, A. (2016). Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie. *Zeitschrift für das gesamte Kreditwesen, 69* (22). S. 35-39.

BOTT, J./MILKAU, U. (2016). Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments. *Journal of Payment Strategy & Systems, Vol. 10* (2). S. 153-171.

V. Rutz, *Blockchain quo vadis*, BestMasters,
https://doi.org/10.1007/978-3-658-29405-2

BOTT, J./MILKAU, U. (2017). Central bank money and blockchain: A payments perspective. *Journal of Payment Strategy & Systems, Vol. 11* (2). S. 145-157.

BRADBURY, D. (2013). The problem with Bitcoin. *Computer Fraud & Security* (11). S. 5-8.

BRÜHL, V. (2017a). Bitcoin und andere Kryptowährungen – konsequente Regulierung und Aufsicht sind dringend geboten. *ifo Schnelldienst, 70. Jg.* (22). S. 13-16.

BRÜHL, V. (2017b). Bitcoins, Blockchain und Distributed Ledgers. *Wirtschaftsdienst* (2). S. 135-142.

BRÜHL, V. (2017c). Virtual Currencies, Distributed Ledgers and the Future of Financial Services. *Intereconomics, Vol. 52* (6). S. 370-378.

Bundesbank. (2017a). Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potenziale und Risiken. *Monatsbericht September 2017, Jg. 69* (9). S. 35-47. Verfügbar unter https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichte/2017/2017_09_monatsbericht.pdf?__blob=publicationFile Zugriff am 14.03.2018.

Bundesbank. (2017b). *Geld und Geldpolitik,* Deutsche Bundesbank. Verfügbar unter https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Schule_und_Bildung/geld_und_geldpolitik.pdf?__blob=publicationFile Zugriff am 12.03.2018.

BURGWINKEL, D. (2016). Blockchaintechnologie und deren Funktionsweise verstehen. In D. Burgwinkel (Hrsg.), *Blockchain Technology. Einführung für Business- und IT Manager* (S. 3-50). Berlin, Boston: De Gruyter Oldenbourg.

BUTERIN, V. (2018). *Meta: cap total ether supply at ~120 million #960*. Verfügbar unter https://github.com/ethereum/EIPs/issues/960 Zugriff am 23.04.2018.

CASTRO, M./LISKOV, B. (1999). Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Desing and Implementation.* Verfügbar unter http://pmg.csail.mit.edu/papers/osdi99.pdf

COCCO, L./MARCHESI, M. (2016). Modeling and Simulation of the Economics of Mining in the Bitcoin Market. *PLoS ONE, Vol. 11* (10). S. 1-31.

Coinmarketcap. (2018). *Kryptowährung Marktkapitalisierungen*. Verfügbar unter https://coinmarketcap.com/de/ Zugriff am 16.03.2018.

DEUBEL, M./MOORMAN, J./HOLOTIUK, F. (2017). Nutzung der Blockchain-Technologie in Geschäftsprozessen: Analyse am Beispiel des Zahlungsverkehrs. In M. Eibl & M. Gaedke (Hrsg.), *Informatik 2017. Tagung vom 25.-29. September 2017 in Chemnitz* (GI-Edition Proceedings, Bd. 275, S. 829-842). Bonn: Gesellschaft für Informatik.

DUPONT, J./SQUICCIARINI, A. C. (2015). Toward De-Anonymizing Bitcoin by Mapping Users Location. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy.* S. 139-141.

EBA. (2013). *EBA/WRG/2013/01 - Warning to consumers on virtual currencies,* European Banking Authority. Verfügbar unter https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf Zugriff am 23.04.2018.

EFANOV, D./ROSCHIN, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science, Vol. 123.* S. 116-121.

ESMA. (2016). *The Distributed Ledger Technology Applied to Securities Markets - Discussion Paper,* European Securities and Markets Authority. Verfügbar unter https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

Etherscan. (2018). *Ethereum Network HashRate Growth Chart*. Verfügbar unter https://etherscan.io/chart/hashrate Zugriff am 21.04.2018.

EYAL, I./SIRER, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In N. Christin & R. Safavi-Naini (Eds.), *Financial cryptography and data security. 18th international conference, FC 2014, Christ Church, Barbados, March 3 - 7, 2014 ; revised selected papers* (Lecture Notes in Computer Science, vol. 8437, pp. 436-454). Heidelberg: Springer.

EZB. (2016a). Distributed Ledger Technology. *IN FOCUS* (1).

EZB. (2016b). *Zahlungsverkehrsstatistik für das Berichtsjahr 2015,* Europäische Zentralbank. Verfügbar unter https://www.bundesbank.de/Redaktion/DE/Downloads/Presse/EZB_Pressemitteilungen/2016/2016_09_26_zahlungsverkehr.pdf?__blob=publicationFile Zugriff am 23.04.2018.

EZB. (2017a). *Guide to fit and proper assessments,* Europäische Zentralbank. Verfügbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.fap_guide_201705.en.pdf Zugriff am 23.04.2018.

EZB. (2017b). *Zahlungsverkehrsstatistik für das Berichtsjahr 2016,* Europäische Zentralbank. Verfügbar unter https://www.bundesbank.de/Redaktion/DE/Downloads/Presse/EZB_Pressemitteilungen/2017/2017_09_15_zahlungsverkehr.pdf?__blob=publicationFile Zugriff am 23.04.2018.

EZB/BOJ. (2017). *Payment systems: liquidity saving mechanisms in a distributed ledger environment,* Europäische Zentralbank; Bank of Japan. Verfügbar unter https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf Zugriff am 23.04.2018.

FAIRLEY, P. (2017). Blockchain World - Feeding the Blockchain Beast. If Bitcoin ever goes mainstream the electricity needed to sustain it will be enormous. *IEEE Spectrum, 54* (10). S. 38-60.

FORMANN, M. (2017). Globale Innovationsinitiative im Zahlungsverkehr und DLT. *Zeitschrift für das gesamte Kreditwesen, 70* (11). S. 551-552.

FREUND, A. (2017). Economic incentives and Blockchain security. *Journal of Securities Operations & Custody, Vol. 10* (1). S. 67-76.

FRIEDMAN, M. (1999). *Interview on Anti-Trust and Tech*. Verfügbar unter https://www.youtube.com/watch?v=mlwxdyLnMXM Zugriff am 23.04.2018.

GEILING, L. (2016). Distributed Ledger. Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain. *BaFinJournal* (2). S. 28-32.

GENCER, A. E./BASU, S./EYAL, I./VAN RENESSE, R./SIRER, E. G. (2018). Decentralization in Bitcoin and Ethereum Networks. Verfügbar unter https://arxiv.org/pdf/1801.03998.pdf Zugriff am 23.04.2018.

GRAMOLI, V. (2017). From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems*. S. 1-10.

GREENSPAN, G. (2016). Payment and exchange transactions in shared ledgers. *Journal of Payment Strategy & Systems, Vol. 10* (2). S. 172-180.

HELDT, C./METZGER, J. (2018). *Settlement*. Verfügbar unter https://wirtschaftslexikon.gabler.de/definition/settlement-44619/version-267925 Zugriff am 23.04.2018.

HERRMANN, G./MÜLLER, D. (2004). *ASIC - Entwurf und Test. Mit 17 Tabellen*. Leipzig: Fachbuchverl. Leipzig im Carl-Hanser-Verl.

HILEMAN, G./RAUCHS, M. (2017). *Global blockchain benchmarking study 2017*. Verfügbar unter https://fsinsights.ey.com/big-issues/Digital-and-connectivity/Global-Blockchain-Benchmarking-Study Zugriff am 28.12.2017.

HOFMANN, E./STREWE, U. M./BOSIA, N. (2018). *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation* (SpringerBriefs in Finance). Cham: Springer International Publishing.

HORVÁTH, P. (2012). *Controlling* (Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften, 12., vollst. überarb. Aufl.). München: Vahlen.

Hyperledger. (2017). *Hyperledger Architecture, Volume 1,* Hyperledger Architecture Working. Verfügbar unter https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf Zugriff am 23.04.2018.

JENTZSCH, N. (2016). Blockchain: Revolution der Finanzwelt? *DIW Wochenbericht* (29). S. 656.

JUNG, R./PLAZIBAT, A. (2017). Blockchain: Heiliger Gral oder überbewerteter Hype? Erkenntnisse aus der Finanzindustrie. *Controlling, 29* (Sonderheft: K). S. 46-51.

KANNENBERG, A. (2018). *Kryptogeld: Bitmain kündigt ersten ASIC-Miner für Ethereum an*. Verfügbar unter https://www.heise.de/newsticker/meldung/Kryptogeld-Bitmain-kuendigt-ersten-ASIC-Miner-fuer-Ethereum-an-4010449.html Zugriff am 23.04.2018.

KAŞKALOĞLU, K. (2014). Near Zero Bitcoin Transaction Fees Cannot Last Forever. In V. Snasel (Ed.), *The International Conference on Digital Security and Forensics (DigitalSec2014), June 24 - 26, 2014* (pp. 91-99). Wilmington, Del.: Society of Digital Information and Wireless Communications (SDIWC).

KAUPP, F./GIERA, E. (2017). Zahlungsverkehr: vom Überweisungsträger zu Instant Payments. In V. Brühl & J. Dorschel (Hrsg.), *Praxishandbuch Digital Banking* (1. Auflage 2018, S. 227-258). Wiesbaden: Springer Fachmedien Wiesbaden GmbH.

KIENZLER, R. (2016). Hyperledger – eine offene Blockchain Technologie. In D. Burgwinkel (Hrsg.), *Blockchain Technology. Einführung für Business- und IT Manager* (S. 111-122). Berlin, Boston: De Gruyter Oldenbourg.

Kraken. (o. J.). *How long do digital assets/cryptocurrency deposits take?* Verfügbar unter https://support.kraken.com/hc/en-us/articles/203325283-How-long-do-cryptocurrency-deposits-take- Zugriff am 23.04.2018.

KUO, T.-T./KIM, H.-E./OHNO-MACHADO, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24* (6). S. 1211-1220.

LAMPORT, L./SHOSTAK, R./PEASE, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, Vol. 4* (3). S. 382-401.

LI, X./JIANG, P./CHEN, T./LOU, X./WEN, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems.* S. 1-13.

LIU, A. (2015). *Implementing the Interledger Protocol in Ripple,* Ripple. Verfügbar unter https://ripple.com/insights/implementing-the-interledger-protocol/ Zugriff am 23.04.2018.

MAINELLI, M./MILLNE, A. (2016). *The Impact and Potential of Blockchain on the Securities Transaction Lifecycle,* SWIFT Insitute. Verfügbar unter https://swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL-1.pdf Zugriff am 23.04.2018.

MARQUER, S. (2017). *XRP Ledger Decentralizes Further With Expansion to 55 Validator Nodes*. Verfügbar unter https://ripple.com/insights/xrp-ledger-decentralizes-expansion-55-validator-nodes/ Zugriff am 28.02.2018.

MEIKLEJOHN, S./POMAROLE, M./JORDAN, G./LEVCHENKO, K./MCCOY, D./VOELKER, G. M./SAVAGE, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the 2013 conference on Internet measurement conference.* S. 127-140.

MESCH, S./JONIETZ, C./PETERS, A. (2017). *ibi Bitz Digital Banking 2017 Q1 Blockchain,* ibi Research an der Universität Regensburg. Verfügbar unter http://www.ibi.de/tmp/9f6e15a75b5c20b03bd610f3ee71a3d934129b4e/ibi_Blitz_2017_Q1_-_Blockchain.pdf Zugriff am 23.02.2018.

METI. (2016). *Survey on Blockchain Technologies and Related Services. FY2015 Report,* Ministry of Economy, Trade and Industry. Verfügbar unter http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf Zugriff am 09.02.2018.

METZGER, J./HELDT, C./HÖLSCHER, R. (2018). *Clearing*. Verfügbar unter https://wirtschaftslexikon.gabler.de/definition/clearing-31574/version-255130 Zugriff am 23.04.2018.

MICHAELIS, J. (2017). Die Konkurrenz umarmen:. *ifo Schnelldienst, 70. Jg.* (22). S. 17-19.

MILKAU, U. (2017). Blockchain in der Kreditwirtschaft: Was ist denkbar? *Zeitschrift für das gesamte Kreditwesen, 70* (11). S. 23-26.

MISHKIN, F. S. (2016). *The economics of money, banking, and financial markets* (Always learning, 11th edition, global edition). Boston: Pearson.

MOORE, T./CHRISTIN, N./SZURDI, J. (2016). *Revisiting the Risks of Bitcoin Currency Exchange Closure*. Verfügbar unter https://tylermoore.utulsa.edu/toit17.pdf Zugriff am 23.04.2018.

MORABITO, V. (2017). *Business Innovation Through Blockchain. The B³ Perspective*. Cham: Springer International Publishing.

MORI, T. (2016). Financial technology: Blockchain and securities settlement. *Journal of Securities Operations & Custody, Vol. 8* (3). S. 208-217.

MÖSER, M./BÖHME, R./BREUKER, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit (eCRS), 2013*. Verfügbar unter https://ieeexplore.ieee.org/document/6805780/ Zugriff am 23.04.2018.

NAKAMOTO, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Verfügbar unter https://bitcoin.org/bitcoin.pdf Zugriff am 27.02.2018.

NARAYANAN, A./BONNEAU, J./FELTEN, E./MILLER, A./GOLDFEDER, S. (2016). *Bitcoin and cryptocurrency technologies. A comprehensive introduction*. Princeton: Princeton University Press.

NEYER, G./GEVA, B. (2017). Blockchain and payment systems: What are the benefits and costs? *Journal of Payments Strategy & Systems, Vol. 11* (3). S. 215-225.

NEYER, G./HUTCHISON, S./PORATH, M. (2016). *Five Things Blockchain Must Get Right to Realize Its Full and Transformative Potential. White Paper*. Verfügbar unter https://www.dh.com/resources/white-papers/five-things-blockchain-must-get-right-realize-its-full-and-transformative Zugriff am 17.12.2017.

OSSINGER, J. (2018). *Roubini Says Bitcoin Is the 'Biggest Bubble in Human History',* Bloomberg. Verfügbar unter https://www.bloomberg.com/news/articles/2018-02-02/roubini-says-bitcoin-is-the-biggest-bubble-in-human-history Zugriff am 13.03.2018.

PAAR, C./PELZL, J. (2016). *Kryptografie verständlich. Ein Lehrbuch für Studierende und Anwender* (eXamen.press). Berlin: Springer Vieweg.

PARK, J. H./PARK, J. H. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry, Vol. 9* (164). S. 1-13. Verfügbar unter http://www.mdpi.com/2073-8994/9/8/164 Zugriff am 23.04.2018.

PETRLIC, R./SORGE, C. (2017). *Datenschutz. Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*. Wiesbaden: Springer Vieweg.

PILKINGTON, M. (2016). Blockchain technology: principles and applications. In F.-J. Olleros & M. Zhegu (Eds.), *Research handbook on digital transformations* (Research handbooks in business and management series, pp. 225-253). Cheltenham, UK: Edward Elgar Publishing.

PINNA, A./RUTTENBERG, W. (2016). Distributed ledger technologies in securities post-trading. Revolution or evolution? *ECB Occasional Paper* (172).

PLOOM, T. (2016). Blockchains - wichtige Fragen aus IT-Sicht. In D. Burgwinkel (Hrsg.), *Blockchain Technology. Einführung für Business- und IT Manager* (S. 123-148). Berlin, Boston: De Gruyter Oldenbourg.

Quandl. (2018). *Bitcoin Hash Rate*. Verfügbar unter https://www.quandl.com/data/BCHAIN/HRATE-Bitcoin-Hash-Rate Zugriff am 21.04.2018.

RAMBURE, D./NACAMULI, A. (2008). *Payment systems. From the salt mines to the board room* (Palgrave Macmillan studies in banking and financial institutions, 1. publ). New York u.a.: Palgrave Macmillan.

Ripple. (o. J.a). *History Sharding,* Ripple. Verfügbar unter https://ripple.com/build/history-sharding/#history-sharding Zugriff am 23.04.2018.

Ripple. (o. J.b). *Ripple Validator Setup*. Verfügbar unter https://ripple.com/build/rippled-setup/#operating-rippled-servers Zugriff am 23.04.2018.

Ripple. (2017). *Ripple Solutions Guide,* Ripple. Verfügbar unter https://ripple.com/files/ripple_solutions_guide.pdf Zugriff am 10.02.2018.

ROSNER, M. T./KANG, A. (2016). Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study. *Michigan Law Review, Vol. 114* (4). S. 649-681.

SCHWARTZ, D./YOUNGS, N./BRITTO, A. (2014). *The Ripple Protocol Consensus Algorithm,* Ripple Labs. Verfügbar unter https://ripple.com/files/ripple_consensus_whitepaper.pdf Zugriff am 23.04.2018.

SEIFERT, F. (2002). *Die Wettbewerbspotenziale von Bankmergern. Eine geschäftsfeldspezifische Untersuchung anhand des Resource-based View* (Bankinformatik-Studien, Bd. 9). Heidelberg: Physica-Verlag HD.

SEITZ, S. (2016). Blockchain - Funktionsweise und mögliche Auswirkungen auf die Bankenbranche. In A. Dittrich & T. Egner (Hrsg.), *Trends im Zahlungsverkehr III* (1st ed., S. 165-180). Cologne: Bank-Verlag.

SIXT, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie*. Wiesbaden: Springer Gabler.

SOMPLONSKY, Y./ZOHAR, A. (2018). Bitcoin's Underlying Incentives. *Communications of the ACM, Vol. 61* (3). S. 46-53.

STOMMEL, S. (2017). Blockchain-Ökosysteme. Identitäts- und Zugangsmanagement zur Blockchain und angedockten Ökosystemen. *Datenschutz und Datensicherheit, 41* (1). S. 7-12.

SÜRMELI, J./DER, U./JÄHNICHEN, S./VOGELSANG, A. (2017). Ein Rahmenwerk zur Protokollierung von Transaktionen in Distributed Ledgers. *Informatik-Spektrum, 40* (6). S. 595-601.

SWAN, M. (2015). *Blockchain. Blueprint for a new economy* (Safari Tech Books Online, 1. ed.). Beijing: O'Reilly.

SWIFT. (2016). *SWIFT on distributed ledger technologies,* SWIFT/Accenture. Verfügbar unter https://www.swift.com/resource/swift-distributed-ledger-technologies Zugriff am 17.12.2017.

THIELE, C.-L. (2017). Zwischen Disruption und Spekulation: von Bitcoin, Blockchain und digitalem Geld. *Zeitschrift für das gesamte Kreditwesen, 70* (12). S. 14-17.

THIELE, C.-L. (2018). *Finger weg von Bitcoin. Gastbeitrag in der Frankfurter Allgemeinen Sonntagszeitung am 04.02.2018,* Deutsche Bundesbank. Verfügbar unter https://www.bundesbank.de/Redaktion/DE/Standardartikel/Presse/Gastbeitraege/2018_02_04_thiele_fas.html

THIELE, C.-L./DIEHL, M. (2017). Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten? *ifo Schnelldienst, 70 Jg.* (22). S. 3-6.

TOBIAS, J. (2016). Blockchain in der Finanzbranche - eine disruptive Technologie? *Bank und Markt* (8). S. 37-39.

TURBAN, E./OUTLAND, J./KING, D./LEE, J. K./LIANG, T.-P./TURBAN, D. C. (2018). *Electronic Commerce 2018 : A Managerial and Social Networks Perspective* (Ninth Edition). Cham: Springer.

VANDEZANDE, N. (2017). Virtual Currencies under EU anti-money laundering law. *Computer Law & Security Review, Vol. 33* (3). S. 341-353.

VUKOLIĆ, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch & D. Kesdoğan (Eds.), *Open problems in network security* (Lecture notes in computer science Security and cryptology, vol. 9591, pp. 112-125). Cham: Springer.

WÖHE, G./DÖRING, U. (2010). *Einführung in die allgemeine Betriebswirtschaftslehre* (Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften, 24., überarb. und aktualisierte Aufl.). München: Vahlen.

World Economic Forum. (2015). *Deep Shift. Technology Tipping Points and Societal Impact* (Survey Report, September 2015), World Economic Forum. Verfügbar unter http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf Zugriff am 02.03.2018.

Xorbin. (2018). *SHA-256 hash calculator*. Verfügbar unter http://www.xorbin.com/tools/sha256-hash-calculator Zugriff am 23.04.2018.

XU, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation, Vol. 2* (25). S. 1-9.

YERMACK, D. (2017). Corporate Governance and Blockchains. *Review of Finance, Vol. 21* (1). S. 7-31.

YLI-HUUMO, J./KO, D./CHOI, S./PARK, S./SMOLANDER, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE, Vol. 11* (10). S. 1-27.

ZAMANOV, A. R./EROKHIN, V. A./FEDOTOV, P. S. (2018). ASIC-resistant Hash Functions. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus).* S. 394-396.