Master Thesis

Blockchain und Kryptowährungen: Ein umfassender ökonomischer Überblick

Emre Ilhan

Betreut von:

Prof. Dr. Fabian Schär

Credit Suisse Asset Management Schweiz-Professur für
Distributed Ledger Technology und Fintech
Center for Innovative Finance, Universität Basel

Major in: Finance, Controlling and Banking

Abgabedatum: 20.01.2020

Abstract

Das Themengebiet der Blockchain und Kryptowährungen ist sehr aktuell und ein immer mehr diskutierter Gegenstand der Forschung. Auf die ökonomische Perspektive ausgerichtete Studien sind dabei vergleichsweise noch selten. Die vorliegende Arbeit befasst sich mit der ökonomischen Literatur über die Blockchain und Kryptowährungen, analysiert die aktuell diskutierten ökonomischen Eigenschaften und unterzieht die bestehende Literatur einer kritischen Würdigung. Dabei sind nicht nur wichtige Erkenntnisse für die Zukunft, sondern auch einige Kontroversen festzustellen. Bestehende Studien untersuchen vorwiegend Problemzonen und Grenzen von Bitcoin. Die vorliegende Arbeit zeigt, dass für einige behauptete Probleme bereits Lösungen existieren. Aktuell bestehenden Problemen, wie der begrenzten Skalierbarkeit von Bitcoin, kann durch Second-Layer Lösungen entgegengewirkt werden.

Inhaltsverzeichnis

University of Basel

Center for
Innovative Finance

Plagiatserklärung

Ich bezeuge mit meiner Unterschrift, dass meine Angaben über die bei der Abfassung meiner Arbeit benutzten Hilfsmittel sowie über die mir zuteil gewordene Hilfe in jeder Hinsicht der Wahrheit entsprechen und vollständig sind. Ich habe das Merkblatt zu Plagiat und Betrug vom 22. Februar 2011 gelesen und bin mir der Konsequenzen eines solchen Handelns bewusst.

Buchs, 20.01.2020

Emre Ilhan

1 Einleitung

1.1 Problemstellung

Dank den zunehmenden Fortschritten in der Ära des Internets und den Informations- und Kommunikationstechnologien hat die Gesellschaft in den letzten Jahrzenten viele Innovationen in verschiedensten Bereichen erfahren (Loader und Dutton (2012)). Dies betrifft auch das Gebiet der digitalen Währungen. Besonders Kryptowährungen sind seit der Einführung von Bitcoin im Jahre 2009 immer mehr ins Rampenlicht getreten (Vora (2015); Berentsen und Schär (2017)). Mittlerweile weist Bitcoin eine Marktkapitalisierung von knapp 135 Milliarden US-Dollar auf (CoinMarketCap (2019)) und ist somit die populärste Kryptowährung, die die zugrunde liegende Technologie, die Blockchain, verwendet (Crosby et al. (2016)). Aus diesem Grund wird für die Beschreibung der Blockchain-Technologie in der Literatur oft die Bitcoin-Blockchain herangezogen (beispielsweise in Schlatt et al. (2016)). Auch in der vorliegenden Arbeit werden viele ökonomische Aspekte in Bezug auf Kryptowährungen mit dem Bitcoin-System erläutert.

Das Bitcoin-System erlaubt es, Transaktionen komplett dezentral, also ohne jegliche Intermediäre abzuwickeln (Nakamoto (2008)). In der Blockchain werden alle vergangenen Transaktionen durch die Teilnehmer des Netzwerks chronologisch registriert, wobei für die Validierung und Aufnahme einer Transaktion in die Blockchain eine anspruchsvolle, rechenintensive kryptografische Aufgabe zu lösen ist. Um Transaktionen als gültig einstufen und den Block in die Blockchain hinzufügen zu können, muss also ein gewisser Aufwand erbracht werden (Badev und Chen (2014)). Dieser Aufwand wird als *Proof-of-Work* bezeichnet. Durch diesen Konsensmechanismus sollen missbräuchliche Handlungen, wie die Aufnahme nicht legitimer Transaktionen in die Blockchain, verhindert werden (Schlatt et al. (2016)). Das Bitcoin-Konzept ermöglicht laut Berentsen und Schär (2017) die kompetitive Schöpfung, virtuelle Darstellung und dezentrale Abwicklung von Werteinheiten.

Aus diesen ersten Eindrücken scheint hervorzugehen, dass die Technologie vor allem transaktionale Vorteile mit sich bringt. Berentsen und Schär (2017, S. 47) reden hierbei über «eine neue Kombination der Kontrollstrukturen», welche «die transaktionalen Vorteile einer virtuellen Geldeinheit mit der systemischen Unabhängigkeit der dezentralen Transaktionsabwicklung verbindet». Jedoch werden einige Eigenschaften von Kryptowährungen nicht selten als kontrovers betrachtet. Chiu und Koeppl (2017) betonen beispielsweise, dass die Erleichterung illegaler Transaktionen durch die Nutzung von Kryptowährungen eine Debatte ist. Böhme et al. (2015) zeigen zunächst die Vorteile von Bitcoin auf, um anschliessend auf die Grenzen aufmerksam zu machen. Dabei stehen verschiedene Risiken sowie regulatorische Aspekte im Vordergrund. Die ökonomische Literatur zum Thema Blockchain und Kryptowährungen wird aufgrund der Aktualität der Thematik immer umfangreicher. Trotzdem besteht ein Bedarf an Forschung, um Probleme aufzuzeigen, die hauptsächlich ökonomischer Natur sind. Die vorliegende Arbeit beschäftigt sich deshalb vorwiegend mit ökonomischen Aspekten. Von vergangenen Studien erwähnte Probleme und Grenzen sollen nicht bloss hingenommen, sondern hinterfragt und gleichzeitig kritisch bewertet werden.

1.2 Zielsetzung

Das Ziel dieser Arbeit ist es, den aktuellen Forschungsstand zum Thema Blockchain und Kryptowährungen aus einer ökonomischen Perspektive darzulegen, indem dem Leser zunächst ein Gesamtüberblick über die bisherige Literatur verschaffen wird. Danach sollen die verschiedenen ökonomischen Modelle in zwei interessanten Papieren im Detail mathematisch sowie intuitiv analysiert, Stärken und Schwächen aufgezeigt und somit neue Erkenntnisse in dieser sehr aktuellen Thematik geschaffen werden. Die vorliegende Arbeit liefert einen Beitrag zur Forschung, indem ökonomische Aspekte und Modelle systematisch und kritisch beurteilt werden. Die ökonomische Literatur wird in einem grossen Umfang zusammengefasst, wobei zwei ausgewählte Studien detaillierter unter die Lupe genommen werden. Ein solcher Ansatz zur Analyse der Thematik existiert

Stand heute und in dem Umfang noch nicht.

1.3 Aufbau der Arbeit

Zunächst werden ökonomische Aspekte zu Blockchain und Kryptowährungen in einer Literaturübersicht zusammengestellt, wobei vorwiegend auf die Bitcoin-Mikrostruktur und damit zusammenhängende Grenzen eingegangen wird. Anschliessend folgt eine detailliertere Analyse von zwei interessanten Studien. Im fünften Kapitel werden die wichtigsten Erkenntnisse der Arbeit diskutiert. Ein abschliessendes Kapitel fasst das Wichtigste zusammen und rundet die Thematik ab.

2 Methodik

In dieser Arbeit wird ein Systematisches Research Review durchgeführt. Wie in der Einleitung beschrieben, wird zunächst ein Gesamtüberblick über die ökonomische Literatur stattfinden, um anschliessend die aus Sicht des Autors wichtigsten Papiere detailliert zu analysieren. Die Quellen wurden mit Hilfe der Suchmaschine «Google Scholar» beschaffen und anhand der Relevanz bezüglich der ökonomischen Aspekte über die Blockchain und Kryptowährungen ausgewählt.

3 Literaturübersicht

In diesem Teil der Arbeit wird die ökonomische Literatur zum Thema Blockchain und Kryptowährungen zusammengefasst. Dabei wird auf viele verschiedene ökonomische Fragestellungen und Probleme der Technologie eingegangen sowie auf Kontroversen hingewiesen. Können Kryptowährungen als Zahlungsmittel funktionieren und den Handel erleichtern? An welche ökonomischen Grenzen stossen Bitcoin und die Blockchain? Welche Faktoren lösen Preisunterschiede aus? Welche Hindernisse können die Vollendung einer Transaktion (*payment finality*) verzögern? Welche Risiken birgt die Bitcoin-Architektur? Solche und ähnliche Fragestellungen wirft die jüngste Literatur auf. Da der Fokus dieser Arbeit auf der ökonomischen Perspektive liegt, werden technische Grundlagen über die Blockchain und Kryptowährungen nicht behandelt.

3.1 Eignung als Zahlungsmittel

Eine Frage bezüglich Kryptowährungen ist deren Eignung als Zahlungsmittel. Dieser Frage gehen Chiu und Koeppl (2017) nach. Sie entwickeln ein Modell, um zu zeigen, dass eine gut konzipierte Kryptowährung Transaktionen sehr wohl vereinfachen und die in der aktuellen Form von Bitcoin sehr hohen Wohlfahrtsverluste senken kann. Eine Herausforderung ist laut den Autoren das *Double-Spending*-Problem. Um dieses Problem zu umgehen, kann der Verkäufer bei einer Transaktion die Lieferung des Gutes so lange verzögern, bis die Zahlung definitiv in die Blockchain aufgenommen wird. Dieses Prinzip wird als *Confirmation Lag* oder *Delivery Lag* bezeichnet. Somit wird der Verkäufer verhindern können, dass er das Produkt zwar geliefert hat, die Zahlung aber nicht erhält. Chiu und Koeppl (2017) beschäftigen sich weiter mit der Frage, welche Anreize das Design einer Kryptowährung bei den Transaktionspartnern schafft. Dabei geht es um Anreize, das System zu attackieren, wie es beim Double-Spending-Problem der Fall ist. Double-Spending kann einerseits durch den oben erwähnten ressourcenintensiven Mining-Prozess und andererseits dem eben angesprochenen Confirmation Lag erschwert

werden. Chiu und Koeppl (2017) untersuchen die Kosten der Anwendung einer Bitcoin-Struktur, die Double-Spending grundsätzlich verbietet. So kann Bitcoin in Bezug auf die Effizienz und Eignung mit bestehenden Zahlungsmitteln verglichen werden.

In der erwähnten Studie kommen die Autoren kommen zum Schluss, dass Bitcoin in Bezug auf Wohlfahrtsverluste um das 500-fache an Kosten gegenüber traditionellen Währungen verursacht und dies dem suboptimalen Design der Kryptowährung geschuldet ist. Gemeint ist damit die Art der Belohnung der Bitcoin-Miner. Diese werden einerseits mit den neu geschöpften Bitcoins[1], andererseits aber auch mit den Transaktionsgebühren entschädigt. Dies ist zu ressourcenaufwändig. Die ausschliessliche Belohnung durch neu geschöpfte Bitcoins würde den Wohlfahrtsverlust beträchtlich reduzieren (Chiu und Koeppl (2017)). Für das Vertrauen in eine Kryptowährung ist die Wechselwirkung zwischen der Sicherheit der Blockchain, die Güte des Mining-Systems und der Wert der Währung von Bedeutung. Chiu und Koeppl (2017) untersuchen in ihrem Modell, wie diese Grössen – der Mining-Aufwand, die Belohnungsstruktur sowie der Wert der Kryptowährung – im Gleichgewicht aussehen.

Im Fall Bitcoin ist es möglich, durch weniger Mining und der exklusiven Belohnung der Miner über neu geschaffene Coins die Wohlfahrtsverluste von 1.4% auf 0.8% des Konsums zu senken (Chiu und Koeppl (2017)). An dieser Stelle kann die Frage gestellt werden, ob die ausschliessliche Belohnung durch neu geschöpfte Bitcoins Sinn macht, zumal diese aufgrund der periodischen Halbierung schliesslich ohnehin gänzlich wegfallen werden. Eine genauere Betrachtung zeigt, dass Transaktionsgebühren notwendig sind.

Da die Transaktionsgebühren einen kleinen Anteil an der gesamten Belohnung haben, sinkt der Anreiz für die Miner, weitere Transaktionen hinzuzufügen, weil diese die Gesamtbelohnung im Vergleich zu den Coin Rewards nur geringfügig beeinflussen (Berentsen und Schär (2017)). Die Gefahr, die Belohnung an einen anderen Miner zu verlieren, der an einem kleineren Block arbeitet und somit schneller zu verbreiten ist, steigt, je

[1] In der vorliegenden Arbeit kurz als *Coin Rewards* bezeichnet.

mehr Transaktionen dazukommen und reduziert Mining-Anreize umso mehr. Deshalb muss der Anteil der Transaktionsgebühren steigen. Dies kann entweder durch deutlich höhere Transaktionsgebühren oder durch die weitere Reduktion der Coin Rewards sichergestellt werden (Berentsen und Schär (2017)). Alternativ kann auch die maximale Blockgrösse ausgedehnt werden, um die Transaktionsgebühren auf mehr Blocks zu verteilen und somit zu erhöhen (Berentsen und Schär (2017)). Um die richtigen Anreize für die Miner setzen zu können, sind die Transaktionsgebühren essenziell.

Wichtig sind Transaktionsgebühren auch hinsichtlich der Verhinderung von *Distributed Denial-of-Service* Angriffen (DDoS)[2]. Dies lässt sich beispielsweise anhand der neuen Form von DDoS Angriffen gegen *Memory Pools* (kurz Mempool) aufzeigen. Im Mempool werden Transaktionen gespeichert, die auf die Bestätigung der Miner warten. Wenn mehr Transaktionen dazukommen, als das Netzwerk bewältigen kann, bildet sich ein Rückstau und die Gefahr, dass lange Zeit im Mempool verbliebene Transaktionen abgelehnt werden. Dies erhöht die Transaktionsgebühren, weil die Nutzer eine Ablehnung ihrer Transaktionen verhindern wollen. Angreifer können durch die Initiierung unnötiger Transaktionen (*dust transactions*) den Mempool überlasten, was Angriffe wie Double-Spending begünstigt (Saad et al. (2018)).

Es werden zwei Ansätze zur Verhinderung solcher DDoS Angriffe unterschieden. Einer davon basiert auf Transaktionsgebühren (*fee-based design*), was die Wichtigkeit der Transaktionsgebühren als Gegenargument zu Chiu und Koeppl (2017) aufzeigt. Dabei werden nur diejenigen Transaktionen akzeptiert, deren Aufnahme in die Blockchain vom Initianten auch wirklich gewünscht werden. Transaktionen, die lediglich zur Überlastung des Mempools initiiert wurden, werden aussortiert. Dies gelingt, indem eine Transaktion vom Mempool nur dann akzeptiert wird, wenn sowohl die minimale Gebühr für die Weiterleitung der Transaktion an andere Knoten (*minimum relay fee*), als auch die Mining-Gebühr gezahlt

[2]DDoS Angriffe haben zum Ziel, die Server der gegnerischen Mining Pools durch unnötigen Verkehr zu verlangsamen (Johnson et al. (2014)).

werden (Saad et al. (2018)).

Somit muss ein Angreifer höhere Gebühren in Kauf nehmen, welche in einem inversen Verhältnis zur Anzahl Transaktionen stehen, die der Angreifer generieren kann. Je höher die Gebühr, die der Angreifer pro Transaktion zahlen muss, umso weniger Transaktionen kann er also aufgrund seines gesunkenen Budgets initiieren. Ein Nachteil des auf Transaktionsgebühren basierenden Ansatzes ist hingegen, dass aufgrund der erhöhten Mining-Gebühren nicht nur Angreifer, sondern auch ehrliche Nutzer weniger Transaktionen generieren können. Um diesen Anreizkonflikt zu umgehen, existiert eine weitere Möglichkeit, die als *age-based* Ansatz bezeichnet wird (Saad et al. (2019)). Darauf wird an dieser Stelle jedoch nicht eingegangen, weil lediglich der erste Ansatz von Interesse ist, um die Wichtigkeit der Transaktionsgebühren aufzuzeigen.

Eine weitere Fragestellung seitens Chiu und Koeppl (2017) lautet, ob Kryptowährungen wirklich als Tauschmittel fungieren und bestehende Zahlungssysteme herausfordern oder gar ablösen können. Die Autoren unterstreichen, dass hierfür Probleme bezüglich der Skalierbarkeit angegangen werden sollten und bezeichnen diese als die grösste technische Herausforderung.

Weil im Fall Bitcoin die Blockgrösse limitiert ist und neue Blocks durchschnittlich nur alle zehn Minuten erstellt werden, ist die Anzahl der abgewickelten Transaktionen im Bitcoin-Netzwerk begrenzt. Dies lässt die Bitcoin-Eignung als Tauschmittel in Frage stellen. Hinzu kommt die Tatsache, dass die Bestätigung von Transaktionen eine ähnlich lange Zeit in Anspruch nimmt (Berentsen und Schär (2017)). Auch wenn Berentsen und Schär (2017) Stand 2017 lediglich etwa eine Verdoppelung der Kapazität des Bitcoin-Netzwerks als realistisch betrachteten, wurde bereits zu diesem Zeitpunkt auf mögliche, sich in Entwicklung befindende *Second-Layer* Lösungen wie beispielsweise das *Lightning Network* verwiesen, die Probleme bezüglich der Skalierbarkeit und der Bestätigungszeiten bei Transaktionen lösen können (Berentsen und Schär (2017); Miraz und Donald (2019*b*); Poon und Dryja (2016)). Solche Lösungsansätze wurden von Chiu und Koeppl (2017) nicht thematisiert, obwohl diese zu

Verbesserungen bezüglich der besagten Faktoren beitragen können.

3.2 Vertrauen in die Blockchain-Technologie

In Bezug auf das Vertrauen in die Blockchain-Technologie existieren weitere Untersuchungsansätze. Budish (2018) zeigt ökonomische Grenzen von Bitcoin und der Blockchain auf und bewertet die Bedingungen, die für das Vertrauen in die Technologie erfüllt werden sollen. Das von Nakamoto (2008) veröffentlichte Bitcoin-Zahlungssystem und der dezentrale Charakter werden in Bezug auf das Vertrauen kritisch beurteilt. Das System wirklich vertrauenswürdig zu gestalten, impliziert laut Budish (2018) hohe Kosten. Die Menge an Rechenleistung, die für das Mining aufgewendet wird, muss dabei einerseits eine Nullgewinnbedingung (*zero-profit condition*), andererseits aber auch eine Anreizbedingung erfüllen, die dafür sorgt, dass die Kosten eines Angriffs höher sind als der Nutzen daraus. Die Belohnung an die Miner muss also grösser sein als der Nutzen eines Angriffs, was laut Budish (2018) sehr teuer ist.

Es wird generell angenommen, dass die Wahrscheinlichkeit eines erfolgreichen Angriffs höher ist, falls der Angreifer über die Mehrheit der gesamten Rechenleistung verfügt (*Majority Attack*) (Bitcoin Wiki (2019); Budish (2018)). Gleichzeitig wird aber erwähnt, dass ein Angriff (beispielsweise in Form von Double-Spending) den Wert des eigenen Bitcoin-Bestandes des Angreifers reduziert (Budish (2018)) und einen Anreiz auslöst, den Angriff zu unterlassen: "A miner with more than 50% hash power is incentived to reduce their mining power and refrain from attacking in order for their mining equipment and bitcoin income to retain its value" (Bitcoin Wiki (2019)).

Auch laut Berentsen und Schär (2017, S. 235) ist ein 51% Angriff nicht derart dramatisch: „Ein 51% Angriff kann im schlimmsten Fall eine Transaktion umkehren oder verhindern, dass bestimmte Transaktionen in die Blockchain aufgenommen werden. Mit den entsprechenden Vorsichtsmassnahmen (Abwarten von Bestätigungen) stellen derartige Angriffe aber ein überschaubares Problem dar".

Das Modell in Budish (2018) besagt insgesamt, dass ein Majority Attack stattfinden kann, wenn Bitcoin als Wertspeicher fungieren kann und somit eine ökonomische Wichtigkeit erlangt, wie es beispielsweise bei Gold der Fall ist. Wie bereits angesprochen, spielen jedoch die ökonomischen Grenzen eine wichtige Rolle und stellen in Frage, welche ökonomische Bedeutung Bitcoin überhaupt erlangen kann (Budish (2018)). Berentsen und Schär (2017) erwähnen, dass vor allem die hohen Volatilitäten im Bitcoinpreis für die Wertspeicherfunktion keine gute Voraussetzung darstellen.

3.3 Probleme im Zusammenhang mit Proof-of-Work

Das Double-Spending-Problem und zusammenhängende Aspekte generieren in der Literatur weiteren Diskussionsstoff. Auer (2019) untersucht Kryptowährungen unter dem Gesichtspunkt des Proof-of-Work. Die Profitabilität von Double-Spending aus Sicht eines Angreifers verzögert und verteuert die Bestätigung von Transaktionen. Ausserdem wird die Belohnung der Bitcoin-Miner mehrheitlich durch neu geschöpfte Bitcoin Einheiten finanziert, da nicht genügend Transaktionsgebühren generiert werden können, um die Sicherheit der Transaktionen zu gewährleisten (Auer (2019)). Das Problem ist, dass höhere Transaktionsgebühren die Sicherheit zwar erhöhen würden, der Anreiz eines einzelnen Nutzers, sich mit der eigenen Gebühr zu beteiligen, jedoch gering ist. Die gesetzte Transaktionsgebühr fällt für jeden Nutzer individuell an, wobei der generierte Nutzen - durch eine höhere Sicherheit der Transaktionen in einem Block - allen Nutzern zugute kommt (Auer (2019)). Transaktionsgebühren tragen vergleichsweise einen sehr geringen Anteil zur gesamten Belohnung der Miner bei (Berentsen und Schär (2017)). Die Tatsache, dass neu geschöpfte Bitcoin Einheiten die Mehrheit der Belohnug ausmachen und nicht genügend Transaktionsgebühren generiert werden können, wird eine Reduktion der Bitcoin-Liquidität nach sich ziehen (Auer (2019)). Dies deshalb, weil „die Wachstumsrate der monetären Basis stetig abnimmt und sich asymptotisch einem Nullwert annähert“ sowie nach dem Erreichen der 21 Millionen Grenze keine weiteren Bitcoin Einheiten mehr

geschöpft werden (Berentsen und Schär (2017, S. 255)). Die Belohnung durch neue Coins wird periodisch (etwa alle vier Jahre) halbiert. Die nächste Halbierung steht im Jahr 2020 wieder an (Auer (2019)).

Auer (2019) betont, dass die Bestätigung von Zahlungen Monate in Anspruch nehmen kann, sobald es aus oben genannten Gründen keine Belohnung durch neu geschöpfte Coins mehr geben wird. Um dem entgegenzuwirken, brauche es neue Technologien, die die Vollendung von Transaktionen beschleunigen, oder gar eine alternative Lösung anstelle des Konsensmechanismus des Proof-of-Work. Sogenannte Second-Layer Lösungen wie beispielsweise das Lightning Netzwerk werden als Mittel zur Verbesserung bezüglich der Skalierbarkeit und der Wartezeit bei Transaktionen vorgeschlagen. Gleichzeitig wird aber betont, dass vom Proof-of-Work unbedingt abgewichen werden sollte. In der Detailanalyse wird auf Second-Layer Lösungen genauer eingegangen.

Eine Alternative zum Proof-of-Work stellt der *Proof-of-Stake* dar. Dabei wird ein Konsens erreicht, indem aus einem Pool von Besitzern der Kryptowährung zufällig (aber proportional zum Vermögen an der Währung) ausgewählt wird, wer Transaktionen bestätigen und neue Blocks hinzufügen darf. Diese müssen jedoch einen Teil ihres Vermögens als Sicherheit hinterlegen. Die Gefahr, bei einem Regelverstoss den besicherten Teil des eigenen Vermögens zu verlieren, schreckt Miner davor ab, das System anzugreifen (Auer (2019)). Die Effizienz im Rahmen des Proof-of-Work ist laut Auer (2019) tiefer als in einem solchen dezentralen System zunächst erwartet werden könne. Eine wichtige Frage in diesem Kontext ist, ob alternative Ansätze wie der Proof-of-Stake ohne zentrale Instanz beziehungsweise institutionelle Koordination erfolgreich sein können (Auer (2019)).

Beim Proof-of-Work wird per Konsens die längste bekannte Kette als der aktuelle Zustand akzeptiert. Um eine alternative Kette zur längsten umformen zu können, braucht der Netzwerkteilnehmer über 50% der gesamten Rechenleistung (Berentsen und Schär (2017)). Beim Proof-of-Stake impliziert dieser Prozess hingegen keine Kosten, weil kein Proof-of-Work für das Mining notwendig ist. Die Miner können somit gleichzeitig an ver-

schiedenen Ketten arbeiten und ihre Chance erhöhen, dass eine von ihnen bearbeitete Kette akzeptiert wird und so Transaktionsgebühren abschöpfen. Dieses Problem wird als *Nothing-at-Stake* bezeichnet. Es gibt also kein eindeutiges Kriterium, um die „richtige“ Kette auszuwählen. Dazu wären weitere Koordinationsmechanismen notwendig. Weitere Konsensmechanismen, wie beispielsweise der *Delegated Proof-of-Stake*, setzen an diesem Punkt an und versuchen, anhand von Abstimmmechanismen die Konsensfindung zu beschleunigen (Auer (2019)). Auf Proof-of-Stake und andere Konsensmechanismen wird in dieser Arbeit aber nicht weiter eingegangen, da die Analyse solcher Alternativen fundiert stattfinden sollte.

Unter Berücksichtigung des Status Quo der Technologie sollte das Hauptaugenmerk laut Auer (2019) also nicht darauf gelegt werden, ob traditionelles Geld und das auf zentrale Instanzen angewiesene Finanzsystem komplett dezentralisiert, sondern ob mit Hilfe der Technologie bestehende Systeme optimiert werden können.

3.4 Risikofaktoren und Regulierung

Die Bitcoin-Technologie bietet ohne Frage viele Vorteile. Ihr dezentraler Charakter, also die Unabhängigkeit von zentralen Instanzen und Regulierungen, sowie die höhere Anonymität der Transaktionspartner ermöglichen einen einfacheren, schnelleren und sichereren Zahlungsaustausch als traditionelle Zahlungssysteme (Böhme et al. (2015)). Jedoch bestehen einige Schwachpunkte und Grenzen. Böhme et al. (2015) gehen in ihrer Studie auf verschiedene Risiken und Regulierungsaspekte ein. Ein Aspekt sind sogenannte *Mining Pools*, in denen Ressourcen kombiniert und die Gewinne aufgeteilt werden. Je grösser solche Pools werden und je mehr Mining-Aktivitäten darin konzentriert sind, desto mehr ist der dezentrale Charakter des Systems gefährdet. Dies wiederum ist zentraler Bestandteil für das Vertrauen in Bitcoin. Sobald ein Mining Pool mehr als die Hälfte der Gesamtrechenleistung kontrolliert, wird ein Angriff möglich (Böhme et al. (2015)).

Nachfolgend werden verschiedene Risiken, die Bitcoin laut Böhme et al.

(2015) mit sich bringt, kategorisch angesprochen. Besitzer der Kryptowährung Bitcoin sind einem Marktrisiko ausgesetzt, weil der Wert einer Einheit Bitcoin im Vergleich zu anderen Währungen schwanken kann. Die untenstehende Abbildung 1 zeigt den Wechselkurs zwischen dem US-Dollar und Bitcoin in der Zeitspanne von Januar 2012 bis April 2015. Besonders zwischen Mitte 2013 und Anfang 2015 wurden grosse Schwankungen verzeichnet (Böhme et al. (2015)).

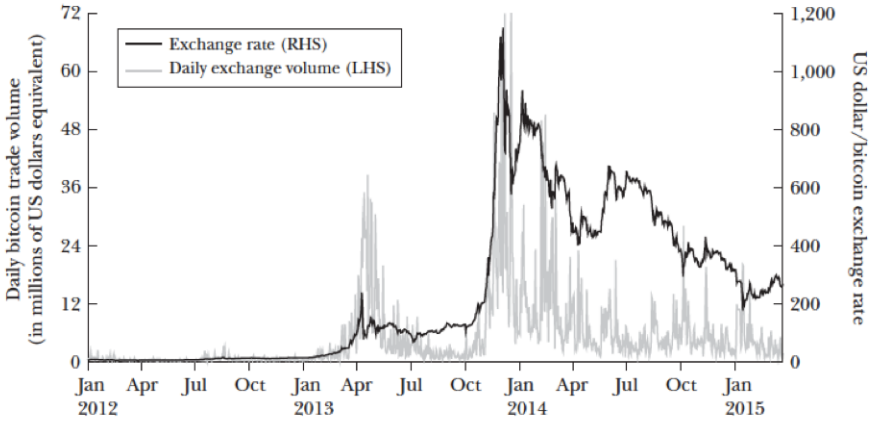

Abbildung 1: Wechselkurs US-Dollar/Bitcoin (Böhme et al. (2015)).

Gründe dafür waren beispielsweise Unsicherheiten im Markt, Medienberichte oder widersprüchliche Aussagen seitens Regulierungs- und Aufsichtsbehörden. Weil die Anzahl der Bitcoins, die im Umlauf sind, begrenzt ist, löst eine hochvolumige Transaktion relativ hohe Wechselkurseffekte aus. Dies stellt eine zusätzliche Ursache für grössere Schwankungen dar (Sixt (2017)). Dass aufgrund des relativ tiefen Handelsvolumens hochvolumige Transaktionen ohne eine gleichzeitge Beeinflussung des Marktpreises erschwert werden, wird als *Shallow Markets* Problem bezeichnet (Böhme et al. (2015)).

Erwähnt wird auch das Gegenparteirisiko. In einer Studie von Moore und Christin (2013) erwies sich rund die Hälfte der untersuchten Tauschgeschäfte zwischen Bitcoin und anderen Währungen als nicht abgeschlossen, in wiederum knapp der Hälfte dieser Transaktionen wurden die Parteien für ihren Verlust nicht entschädigt (Böhme et al. (2015)). Jedoch

existieren bereits Möglichkeiten, Transaktionen zwischen Parteien ohne zentrale Instanz sicher zu gestalten. Atomic Swaps bezwecken, die Interoperabilität zwischen Blockchains[3] und Mängel bezüglich der Skalierbarkeit von Kryptowährungen zu verbessern und dafür zu sorgen, dass keine Partei ihre Coins an das Gegenüber verliert (Lys et al. (2019)). Solche durch das Lightning-Netzwerk ermöglichte *Off-Blockchain* Atomic Swaps werden nicht alle einzeln, sondern aggregiert in der Blockchain verbucht, was eine geringere Belastung der maximalen Blockgrösse mit sich bringt (Berentsen und Schär (2017)). Ausserdem betonen Miraz und Donald (2019*b*), dass dies die Wartezeit bei unbestätigten Transaktionen und somit *On-Blockchain*-Transaktionsgebühren reduzieren wird. Atomic Swaps sind jedoch noch in der Entwicklungsphase, weshalb Stand heute einige Verbesserungspotenziale bestehen. Beispielsweise sind vor allem On-Blockchain Swaps sehr langsam, oder eine nicht vollendete Transaktion ist zwar reversibel, die Rückerstattung jedoch zeitversetzt (Miraz und Donald (2019*a*)). Es soll also nicht behauptet werden, dass Risiken wie das Gegenparteirisiko vollumfänglich verhindert, sondern reduziert werden können.

Der Fakt, dass Bitcoin-Transaktionen nicht rückgängig gemacht werden können, erzeugt laut Böhme et al. (2015) – eben erwähnte Second-Layer Lösungen ausser Betracht gelassen – ein Transaktionsrisiko. Das Fehlen einer zentralen Instanz oder eines Mechanismus, die solche fehlerhafte, ungewollte Transaktionen rückgängig machen könnten, stellt also ein Risiko für die Handelspartner und eine Schwäche von Bitcoin als Zahlungsmittel dar. Hinzu kommt das Risiko, dass eine einst dominante Blockchain diese Eigenschaft verliert und folglich alle Transaktionen in dieser Version der Kette ungültig werden. Auch das sogenannte *Blacklisting* kann einen Risikofaktor darstellen (Böhme et al. (2015)). Berentsen und Schär (2017, S. 175) definieren Blacklisting als „ein Begriff für das Erstellen von Listen, die verschiedene Transaktionsoutputs als ungültig beziehungsweise nicht mehr handelbar erklärt“. Auch wenn die Regulie-

[3]Die Gewährleistung der Interoperabilität zwischen verschiedenen Blockchains ist eine grosse Herausforderung in der Blockchain-Welt. Atomic Swaps sollen Transaktionen zwischen unterschiedlichen Blockchains ohne zentrale Instanz ermöglichen (Lys et al. (2019)).

rung durch Blacklisting plausibel zu sein scheint, impliziert ein möglicher Missbrauch der Blacklist durch die Verantwortlichen – beispielsweise durch bewusste Ablehnung gewisser Transaktionen durch politischen Druck (Möser und Narayanan (2019)) – ein Risiko für die Netzwerkteilnehmer (Böhme et al. (2015)). Die bereits angesprochene Gefahr eines 51%-Angriffs lässt sich der Kategorie der operationellen Risiken einordnen und kann dem Vertrauen in Bitcoin schaden.

Doch Angriffe können auch zwischen den verschiedenen Mining-Pools stattfinden. Das Ziel ist es, den gegnerischen Pool zu benachteiligen und die eigene Chance, das Mining-Rennen zu gewinnen, zu erhöhen. Konkret kann dies einerseits durch Investitionen in die Erhöhung der eigenen Rechenleistung stattfinden. Andererseits besteht für einen Mining-Pool die Möglichkeit, andere Pools direkt anzugreifen. Prominentes Beispiel sind Distributed Denial-of-Service-Angriffe. Diese haben zum Ziel, die Aktivitäten anderer Mining-Pools zu verlangsamen, indem durch einen unnötigen Internetverkehr eine Überlastung der gegnerischen Server verursacht wird (Johnson et al. (2014); Böhme et al. (2015)).

Zu beachten sind gemäss Böhme et al. (2015) auch Risiken bezüglich des Datenschutzes und der Privatsphäre. Genauer betrachtet bietet das System keine perfekte Anonymität (die im Grunde genommen als Vorteil des Systems gilt), da in den Transaktionen Kontoinformationen preisgegeben werden. Gemeint sind damit nicht Name oder Adresse des Nutzers, sondern dessen Public Key. Transaktionen können aber dann auf echte Personen zurückgeführt werden, falls beispielsweise Bitcoins über die Bank in eine andere Währung umgetauscht werden. Somit kann allenfalls die Transaktionshistorie eines Netzwerkteilnehmers rekonstruiert werden (Böhme et al. (2015)). Anhand des Public Keys auf mangelnden Datenschutz zu schliessen, ist jedoch fragwürdig. Der Public Key ist im Vergleich zum Private Key ohnehin nicht geheim zu halten. Die Verwendung eines neuen Schlüsselpaars für jede neue Transaktion würde das Problem bereits beseitigen (Conti et al. (2018)).

Wie sieht die Zukunft von Bitcoin und anderer Kryptowährungen aus? Können wichtige Aspekte wie Dezentralisierung, Schutz der Privatsphäre,

Käufer- und Verkäuferschutz oder die Geschwindigkeit der Transaktionsbestätigungen die Bedürfnisse der Nutzer befriedigen? Das Design des Bitcoin-Systems bietet in der Theorie Antworten auf diese und ähnliche Fragen. In der Praxis scheint jedoch nicht ganz klar zu sein, ob die Bitcoin-Architektur beispielsweise für eine unmittelbare Bestätigung von Transaktionen geeignet ist. Mittlerweile sind viele andere Kryptowährungen entstanden, die in diesen Aspekten effizienter sind. Dass Litecoin in der Transaktionsbestätigung um das Vierfache schneller ist als Bitcoin, oder NXT dank der Nutzung des Proof-of-Stake weniger Ressourcen beansprucht, sind lediglich zwei Beispiele, die auf Probleme und Verbesserungspotenziale der Bitcoin-Architektur hindeuten. Für die Überwindung solcher Hürden sind grundlegende Anpassungen des Bitcoin-Designs notwendig. Die Anpassungsfähigkeit ist aber laut den Autoren die Problemzone von Bitcoin (Böhme et al. (2015)).

Vor allem die Behauptung von Böhme et al. (2015) bezüglich Litecoin ist allerdings kontrovers. Litecoin erzeugt im Schnitt alle 2.5 Minuten einen neuen Block, wobei dieser Schnitt bei Bitcoin bei etwa zehn Minuten liegt. Für die gleiche Sicherheit, die Bitcoin liefert, müssten bei Litecoin jedoch mehr Bestätigungen abgewartet werden. Unter dem Strich ist also der Durchschnitt allein kein Indikator für die Geschwindigkeit und die gleichzeitige Sicherheit der Transaktionen. An den Exchanges ist dieser Unterschied sehr gut zu beobachten. Auch wenn die Anzahl Bestätigungen, die abgewartet werden, je nach Exchange variieren, ist sie bei Bitcoin deutlich tiefer als bei Litecoin. Auf Cryptowelt (2019) werden verschiedene Exchanges diesbezüglich verglichen. Auf der Plattform Bitstamp sind es für Bitcoin beispielsweise drei, für Litecoin hingegen sechs abzuwartende Bestätigungen.

3.5 Delivery Lag und Double-Spending

Eingangs der Literaturübersicht wurde das Double-Spending-Problem angesprochen. Chiu und Koeppl (2017) halten fest, dass dieses Problem unter anderem mittels eines Delivery Lags behoben werden kann. Kang

(2019) greift die Thematik ebenfalls auf und zeigt, dass Double-Spending auch ohne Delivery Lag verhindert werden kann. Hierfür ist jedoch, wie im Modell von Chiu und Koeppl (2017), ein passendes Design der Kryptowährung und der Anreizsysteme notwendig. Kang (2019) entwickelt ein solches Modell und diskutiert Wohlfahrtseffekte eines optimalen Systems. Bitcoins werden in sogenannten *Wallets* gespeichert und über diese gehandelt. Double-Spending-Versuche können überwacht werden und den Ruf einer Wallet beeinflussen. Wenn eine Wallet keine Double-Spending-Versuche zu verzeichnen hat, hat sie einen guten Ruf. Unter der Bedingung, dass der Verlust einer solchen guten Wallet den Nutzen aus einem Double-Spending-Angriff überwiegt, wird ein Nutzer keinen Anreiz haben, über diese Wallet Double-Spending zu betreiben (Kang (2019)). Auch die Schwierigkeit des Minings beeinflusst Double-Spending.

Je schwieriger und aufwändiger das Mining, desto tiefer ist der Anreiz, mit einer guten Wallet Double-Spending zu betreiben. Wenn der Käufer die Zahlung über eine Wallet mit einem schlechten Ruf tätigt, wird er die Ware erst nach der endgültigen Bestätigung der Zahlung und der Aufnahme in die Blockchain erhalten, was den Nutzen aus dem Konsum reduzieren wird. Denn es gilt: Konsum heute ist besser als Konsum morgen. Bei einer Zahlung über eine gute Wallet wird der Verkäufer die Ware sofort liefern. Dann wird Double-Spending nur stattfinden, falls der Nutzen daraus die Kosten des Verlustes der guten Wallet aus Sicht des Käufers übersteigt. Wenn Double-Spending aufgedeckt wird, kann der Angreifer fortan lediglich mit der schlechten Wallet Transaktionen durchführen. Das bedeutet, dass dieser Käufer Kosten und Nutzen eines Angriffs abwägen muss (Kang (2019)).

Zudem sind im Modell von Kang (2019) drei verschiedene Gleichgewichte möglich, die jeweils von den Double-Spending-Anreizen abhängen. Im ersten Gleichgewicht (*delivery lag equilibrium*) sind die Einbussen durch den Verlust einer guten Wallet nicht hoch genug, wodurch der Anreiz für Double-Spending bestehen bleibt. Verkäufer liefern das Gut also erst nach der endgültigen Aufnahme der Zahlung in die Blockchain. Im zweiten Gleichgewicht (*threat of double spending equilibrium*) sind die Einbussen

hoch genug und Double-Spending wird ohne eine verzögerte Lieferung verhindert. Im dritten Gleichgewicht (*no threat of double spending equilibrium*) würden Delivery Lags den Nutzen des Käufers erheblich mindern, wodurch ebenfalls kein Double-Spending stattfindet und die Lieferung unmittelbar durchgeführt wird. Kang (2019) stellt ausserdem fest, dass der Anreiz für Double-Spending über eine gute Wallet negativ mit der Schwierigkeit des Minings korreliert. Je schwieriger der Proof-of-Work, desto länger dauert die Transaktionsbestätigung und die Lieferung der Güter. Je mehr Zeit die Lieferung in Anspruch nimmt, umso weniger lohnenswert ist es, mit einer schlechten Wallet zu handeln. Dieser Zusammenhang reduziert wiederum den Anreiz für Double-Spending mit einer guten Wallet. Bezüglich Wohlfahrt ist laut Kang (2019) das *no threat of double spending*-Gleichgewicht optimal, weil das Handelsvolumen bei diesem Gleichgewicht am höchsten ist.

3.6 Koexistenz von Geld und Bitcoin

Aspekte wie der Mining-Prozess und die Dauer von Transaktionsbestätigungen können weitere Zusammenhänge erklären. Kang und Lee (2019) analysieren die Koexistenz von traditionellem Fiatgeld und Bitcoin als Tauschmittel. Welche Bedingungen dafür erfüllt sein müssen, ob Bitcoin überhaupt mit Fiatgeld konkurrieren kann und welche Wohlfahrtseffekte eine Ökonomie mit oder ohne Koexistenz der beiden Tauschmittel impliziert, wird anhand eines Modells untersucht. Dabei werden sowohl das traditionelle Geld wie auch Bitcoin als Fiatgeld definiert. Ein Unterschied der beiden Tauschmittel ist allerdings, dass bei Transaktionen mit traditionellem Geld Umsatzsteuern auf Verkäufe erhoben werden. Bei Bitcoin-Transaktionen gibt es hingegen keine Steuern, sondern bekanntlich Transaktionsgebühren für die Miner. Die Wohlfahrt in einer Ökonomie, in der es nur traditionelles Geld gibt, ist höher als in einer dualen Ökonomie mit Geld und Bitcoin. Die verzögerte Lieferung im Bitcoin-System, die Double-Spending verhindern soll, führt zu einem Nutzenverlust. Auch der ressourcenaufwändige Mining-Prozess an sich reduziert die Wohlfahrt.

Ob Bitcoin mit traditionellem Geld mithalten und konkurrieren kann, hängt massgeblich von der Höhe der Inflation ab. Eine steigende Inflation reduziert die Wohlfahrt und das Handelsvolumen in beiden Ökonomien, weil der Wert des Geldes sinkt. In der dualen Ökonomie kann jedoch Geld mit Bitcoins substituiert werden. In der Ökonomie mit Geld *und* Bitcoin sinkt das Handelsvolumen folglich weniger stark, weil zwar weniger Transaktionen mit Geld, aber dafür mehr mit Bitcoins stattfinden. In der Summe sinkt das Handelsvolumen in der dualen Ökonomie also weniger als in jener mit ausschliesslich traditionellem Geld. Je mehr Bitcoin-Transaktionen, umso länger dauert wiederum die Transaktionsbestätigung im Durchschnitt. Dies reduziert den effektiven Konsum und folglich die Wohlfahrt in der dualen Ökonomie. Eine steigende Inflation erhöht also die Wohlfahrtsunterschiede zwischen den beiden Ökonomien (Kang und Lee (2019)).

Kang und Lee (2019) untersuchen nebst diesen Zusammenhängen auch den Effekt von höheren Transaktionsgebühren auf die Wohlfahrt. Sie kommen zum Schluss, dass höhere Transaktionsgebühren die Wohlfahrt in der dualen Ökonomie erhöhen. In einer Ökonomie, in der nur Bitcoin als Tauschmittel fungiert, ist das Gegenteil der Fall. Wenn die Transaktionsgebühren steigen, sinkt die Anzahl an Bitcoin-Transaktionen in der dualen Ökonomie. Gleichzeitig gibt es mehr Transaktionen mit traditionellem Geld. Die Käufer substituieren also Bitcoin mit Geld. In der Ökonomie mit Bitcoin als einziges Tauschmittel existiert diese Möglichkeit nicht. Insgesamt steigt in der dualen Ökonomie die Bitcoin-Effizienz (weil es weniger Bitcoin-Transaktionen gibt und dadurch deren Bestätigungsdauer im Durchschnitt sinkt) wie auch die Wohlfahrt (weil Geld als das effizientere Tauschmittel gilt und mehr Transaktionen mit Geld durchgeführt werden) (Kang und Lee (2019)). Eine abschliessende Aussage über die Eignung von Bitcoin als Tauschmittel kann auch an dieser Stelle nicht gemacht werden.

3.7 Internationale Preisunterschiede bei Kryptowährungen

Bisher angesprochene Faktoren wie Transaktionsgebühren oder die Bestätigungsdauer von Transaktionen in der Blockchain können gemeinsam mit anderen Aspekten internationale Preisunterschiede im Bitcoin-Markt erklären. Choi et al. (2018) untersuchen diese Faktoren. Dabei liegt der Fokus auf der sogenannten *Kimchi-Prämie*, die anhand des Preisunterschiedes zwischen dem südkoreanischen und US-amerikanischen Bitcoinmarkt gemessen wird.

Je höher die Belohnung der Miner, desto eher und schneller werden diese eine Transaktion in die Blockchain aufnehmen und auf die Nutzung der Preisunterschiede durch Arbitrage verzichten. Die Unsicherheit, die durch längere Bestätigungszeiten generiert wird, reduziert den Anreiz für Arbitrage ebenfalls. Somit entstehen Preisunterschiede. Der Effekt dieser Faktoren ist für den südkoreanischen Markt jedoch um einiges höher. Der entscheidende Unterschied liegt im Kapitalverkehr. In Ländern, in denen der Kapitalverkehr restriktiver ist, ist Arbitrage teurer. Südkorea ist ein solches Land, das höhere wirtschaftliche Restriktionen aufweist. Die Wechselwirkung zwischen den Prämien und Transaktionsgebühren, Bestätigungszeiten sowie Volatilitäten in der Kryptowährung ist in Südkorea also stärker als beispielsweise in Europa. Zwischen Ländern ohne grosse Kapitalverkehrskontrollen sind die Preisunterschiede vernachlässigbar klein. Dies unterstreicht die Bedeutung, die den Kapitalverkehrskontrollen in Bezug auf die Preisunterschiede zukommt (Choi et al. (2018)). Die untenstehende Abbildung 2 verdeutlicht, dass eine hohe ökonomische Freiheit mit tieferen Preisunterschieden verbunden ist. Die Prämien wurden in Bezug auf den US-Dollar gemessen.

Die Abbildung zeigt eine deutlich negative Korrelation zwischen den Prämien und der ökonomischen Freiheit der jeweiligen Länder. Singapur (SGD) weist beispielsweise eine hohe ökonomische Freiheit und gleichzeitig eine sehr tiefe Bitcoin-Prämie auf, wobei diese für Südkorea (KRW) etwas höher liegt, weil die ökonomische Freiheit geringer ist. In der De-

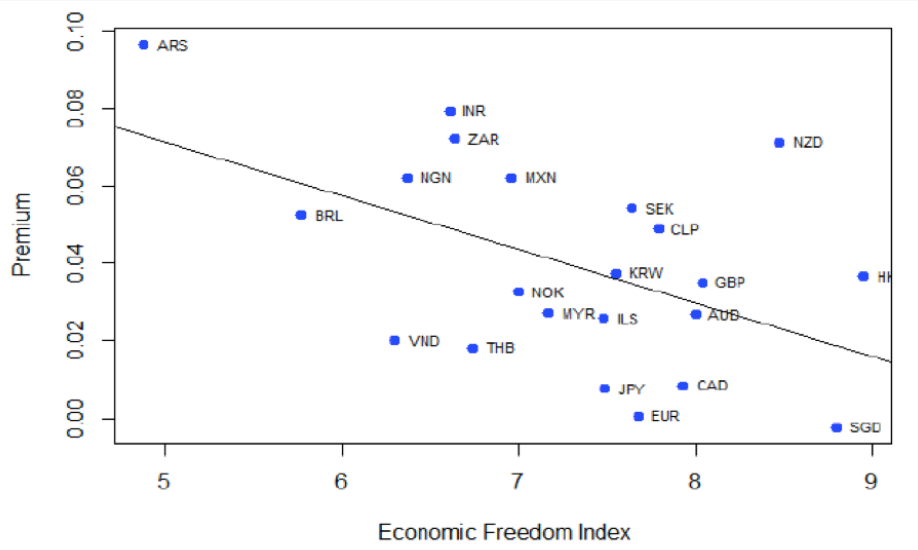

Abbildung 2: Korrelation zwischen Bitcoin-Prämie und ökonomischer Freiheit (Choi et al. (2018)).

tailanalyse im vierten Kapitel werden die Prämien für Kryptowährungen näher betrachtet.

3.8 Abschliessende Bemerkungen

Insgesamt zeigt die bisherige ökonomische Literatur über die Blockchain und Kryptowährungen viele Vorteile eines dezentralen Zahlungssystems, aber auch einige Problemzonen. Im Rahmen der Mikrostruktur von Kryptowährungen werden Mängel bezüglich der Sicherheit, der ökonomischen Effizienz oder der Eignung von Bitcoin als Tauschmittel adressiert. Auch die verschiedenen Konsensmechanismen werden in der aktuellen Literatur diskutiert. Der Proof-of-Stake gilt dabei als weniger ressourcenaufwändig als der Proof-of-Work, das im Bitcoin-System Anwendung findet (Saleh (2019)). Eine hundertprozentige Sicherheit bietet aber auch der Proof-of-Stake nicht. Nebst dem bereits erwähnten Nothing-at-Stake-Problem sind auch sogenannte *Long-Range*-Angriffe möglich, wobei die Historie einer Blockchain gänzlich verändert wird. Die veränderte Kette ist dann von der eigentlichen, richtigen Kette nicht mehr zu unterschei-

den und kann von Nutzern fälschlicherweise anstelle der richtigen Kette verwendet werden (Li et al. (2017)). Es bestehen weitere Konsensmechanismen wie beispielsweise der Delegated Proof-of-Stake oder der Proof-of-Existence. Im Prinzip bringen alle Konsensmechanismen Vor-, aber auch Nachteile mit sich. Der von PeerCoin verwendete Proof-of-Activity beispielsweise macht von den Vorteilen des Proof-of-Work und Proof-of-Stake Gebrauch, wobei trotzdem einige Komponenten der Nachteile der beiden Konsensmechanismen - wie der hohe Ressourcenverbrauch beim Proof-of-Work oder das Nothing-at-Stake Problem beim Proof-of-Stake - verbleiben (Mattila (2016)).

Viele der in dieser Literaturübersicht behandelten Probleme und Grenzen des Systems werden auf die Mikrostruktur der Kryptowährungen zurückgeführt. Dabei wird in diesen Studien oft versucht, ein optimales Design für Kryptowährungen zu finden, um bestehende Probleme reduzieren oder eliminieren zu können. Einige Studien machen teilweise jedoch kontroverse Aussagen, welche bereits in dieser Literaturübersicht dargestellt wurden. Im folgenden vierten Kapitel werden zwei Papiere herangezogen, um ökonomische Aspekte und angedeutete Kontroversen detaillierter zu analysieren.

4 Detailanalyse

Auf Basis der in der Literaturübersicht behandelten Thematiken werden nun die interessantesten zwei Studien detailliert unter die Lupe genommen. Dabei werden die wichtigen Modelle mathematisch und intuitiv erläutert, die Idee der Studien aufgezeigt und kritisch beurteilt, indem die positiven und negativen Aspekte gegenübergestellt werden.

4.1 Beyond the Doomsday Economics of Proof-of-Work in Cryptocurrencies (Auer (2019))

Diese Studie wurde ausgewählt, weil sie unter Einbezug verschiedener Faktoren wie Double-Spending und Transaktionsgebühren interessante ökonomische Grenzen von Kryptowährungen aufzeigt. Ein weiteres Argument ist die Aktualität der Studie. Somit werden Problematiken angesprochen, die aktuell von Bedeutung sind.

4.1.1 Idee der Studie

In der Studie von Auer (2019) wird die Funktionsweise von Kryptowährungen unter dem Gesichtspunkt des Proof-of-Work untersucht. Die Zukunft der auf diesem Konsensmechanismus basierenden Kryptowährungen wird diskutiert. Zentraler Untersuchungsgegenstand ist dabei der Prozess der Transaktionsbestätigung im Bitcoin-System. Eine Zahlung gilt erst als endgültig abgeschlossen, wenn sie nicht mehr rückgängig gemacht und verändert werden kann. Mining impliziert einerseits Kosten, was den Anreiz, das System anzugreifen, reduzieren kann. Andererseits erhalten die Miner für eine korrekte Bearbeitung eine Belohnung in Form von Transaktionsgebühren und neu geschöpften Bitcoins. Auer (2019) analysiert dieses Design einer Kryptowährung.

Konkret wird kritisch beurteilt, ob die Erhöhung der Sicherheit mithilfe einer solchen Kostenstruktur effizient ist und ob die Belohnungsstruktur die richtigen Anreize setzen kann, um Payment Finality sicherzustellen. Das Dilemma liegt in der Tatsache, dass beim Proof-of-Work die Belohnung der Miner genügend hoch sein muss, um die Sicherheit der Transaktionen zu gewährleisten, der Transaktionsmarkt dem jedoch nicht gerecht werden kann. Weil im Fall von Bitcoin die Schöpfung neuer Coins begrenzt ist, wird die Wichtigkeit der zweiten Belohnungskomponente – Transaktionsgebühren – umso mehr steigen. Da der Bedarf an Belohnung nicht gedeckt werden kann, sinkt nebst der Liquidität auch die Sicherheit des Systems. Dieses Szenario führt zu einer erheblichen Verzögerung bei

der Bestätigung von Transaktionen (Auer (2019)).

Auer (2019) diskutiert die ökonomischen Aspekte bezüglich Payment Finality im Bitcoin-System. Entgegen Nakamoto (2008) definiert Auer (2019) eine Zahlung als abgeschlossen, wenn es für potenzielle Angreifer ökonomisch betrachtet nicht mehr lohnenswert ist, Double-Spending zu betreiben. Nakamoto (2008) hingegen besagt, dass ein Angriff umso schwieriger und unwahrscheinlicher wird, je weiter zurück die Zahlung in der Kette liegt. Payment Finality wird also unterschiedlich definiert. Der Ansatz von Auer (2019) wird als *Economic Finality* bezeichnet, derjenige aus Nakamoto (2008) stellt eine operationelle Perspektive dar. Auer (2019) demonstriert mithilfe des ökonomischen Ansatzes, wie teuer und ineffizient es sein kann, um mittels Proof-of-Work die Sicherheit der Zahlungen zu gewährleisten. Dabei wird eine Bedingung definiert, unter welcher ein Angriff nicht lohnenswert ist. Dies ist der Fall, wenn die Kosten eines Angriffs den Nutzen daraus übersteigen. In einem zweiten Schritt wird aufgezeigt, dass sich in einem dezentralen Gleichgewicht eine suboptimale Transaktionsgebühr bildet. Im folgenden Abschnitt wird das formale Vorgehen erläutert.

4.1.2 Analyse des Modells

Eine der Hauptaussagen von Auer (2019) bezieht sich auf die hohen Kosten bei der Gewährleistung der Sicherheit unter Verwendung des Proof-of-Work. Folgende Ungleichung definiert die Bedingung, unter der ein Angriff aus Sicht eines potenziellen Angreifers nicht lohnenswert ist:

$$> \underbrace{\sum_{t \text{ in } b} Amount_t}_{Amount\ that\ is\ double-spent} * \underbrace{\left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash} \frac{P_{USD}}{(1-\Pi^{HF})P_{USD}^{Attack}} - 1\right)^{-1}}_{Attacker\ disadvantage} \quad (1)$$

$$\underbrace{\sum_{i=b}^{i=b+Waittime} Mining\ revenue_i^{BTC}}_{Cost\ of\ a\ forgery}$$

Diese Ungleichung zeigt, dass sich ein Angriff nicht lohnt, wenn die Kosten höher sind als der Nutzen. Die linke Seite stellt die Kosten einerseits in Form des Mining-Einkommens dar, der bei einem Angriff entfällt (neu geschöpfte Coins und Transaktionsgebühren). Andererseits vergrössert sich dieser Term aber auch bei einer hohen Anzahl an Blocks, die gefälscht werden müssen. Zweiteres wird als *Waittime* bezeichnet und in Anzahl Blocks ausgedrückt, bis die Ware geliefert wird. Hinzu kommt ein weiterer Block, da die gefälschte Blockchain länger sein muss als die Richtige. Der erste Faktor auf der rechten Seite der Ungleichung bildet den Transaktionswert in einem Block ab. Je höher der Gesamtwert der Transaktionen, umso grösser ist der Betrag, mit dem ein Angreifer Double-Spending betreiben kann und umso grösser der Anreiz, dies zu tun. Ein hoher Transaktionswert erhöht also die Anfälligkeit auf Angriffe. Der zweite Term beschreibt die Kosten, die dem Angreifer zukommen. Die kurzfristige Beschaffung von Mining-Ressourcen (*cost per rented hash*) verursacht generell höhere Kosten als im Normalfall, wodurch der Quotient ($\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash}$) vermutlich grösser als eins sein wird. Dazu kommt der Quotient, der den Wert von Bitcoin vor und nach einem Angriff misst. Wenn der Wert nach einem Angriff zusammenbricht ($\frac{P_{USD}}{P_{USD}^{Attack}} > 1$), ist der Angreifer negativ davon betroffen. Das Produkt aus den Mining-Kosten und dem Wert von Bitcoin ist in diesem Fall positiv und verkleinert die rechte Seite der Ungleichung. Je mehr der Angreifer also von diesen negativen Einflüssen betroffen ist (*attacker disadvantage*), umso tiefer der Anreiz und die Wahrscheinlichkeit für Double-Spending. Eine Rolle spielt auch die Wahrscheinlichkeit, mit der die Netzwerkteilnehmer eine längste, aber verfälschte Kette ignorieren (Π^{HF}). Dieses Vorgehen wird als *Hard Fork* bezeichnet. Je höher die Wahrscheinlichkeit Π^{HF} ist, desto schwieriger wird ein Angriff.

Unter der Annahme, dass Netzwerkteilnehmer dies nicht tun ($\Pi^{HF} = 0$) und dass das Mining-Einkommen sowie der Transaktionswert konstant sind, kann die Ungleichung (1) folgendermassen umschrieben werden:

$$\underbrace{\frac{Mining\ revenue_b^{BTC}}{\sum_{t\ in\ b} Amount_t}}_{avg.\ transaction\ cost\ in\ \%} > (Wait\ time)^{-1}\left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash} * \frac{P_{USD}}{P_{USD}^{Attack}} - 1\right)^{-1} \quad (2)$$

Falls die Kosten einer kurzfristigen Beschaffung von Mining-Ressourcen wie angenommen höher sind als für ehrliche Miner, die keinen Angriff bezwecken, und der Wert von Bitcoin nach einer Attacke sinkt, wird die Wartezeit für die Aufnahme einer Transaktion in ein Block um ein Vielfaches steigen, je weniger Transaktionsgebühren die Nutzer bereit sind zu zahlen. Dieser Zusammenhang verdeutlicht die hohen Kosten der dezentralen Sicherheitsgewährleistung (Auer (2019)). Auer (2019) hält ausserdem fest, dass die Wartezeit nur linear und nicht etwa exponentiell (wie in Nakamoto (2008)) in die Ungleichung (2) einfliesst. Das bedeutet, dass für eine höhere Sicherheit der Zahlungen sowie für tiefe Transaktionsgebühren entsprechend hohe Wartezeiten in Kauf zu nehmen sind (Auer (2019)).

Dies steht in Verbindung mit der zweiten wichtigen Aussage in der Studie von Auer (2019): Das Bitcoin-System kann nicht genügend hohe Transaktionsgebühren generieren. Eine Ausnahme bildet der Fall, in dem die Blocks bereits die maximale Grösse erreicht haben. Ausstehende Transaktionen landen in diesem Fall in der Warteschlange und ungeduldige Nutzer setzen höhere Transaktionsgebühren, damit ihre Transaktion bevorzugt wird. In einem solchen Szenario können Transaktionsgebühren schlagartig in die Höhe gehen, wie die untenstehende Abbildung 3 zeigt.

Die Blockgrösse wird hier in Megabytes und die Höhe der Transaktionsgebühren in US-Dollar gemessen. Wenn ein Block jedoch genug freie Kapazität aufweist, kann der Miner eine Transaktion ohne zusätzliche marginale Kosten in den Block aufnehmen. In diesem Fall wird jede Transaktion mit einer beliebig positiven Gebühr in den Block aufgenommen. Je nachdem, wie die aktuelle Nachfrage nach Transaktionen und die Blockgrösse aussehen, kann die durchschnittliche Transaktionsgebühr al-

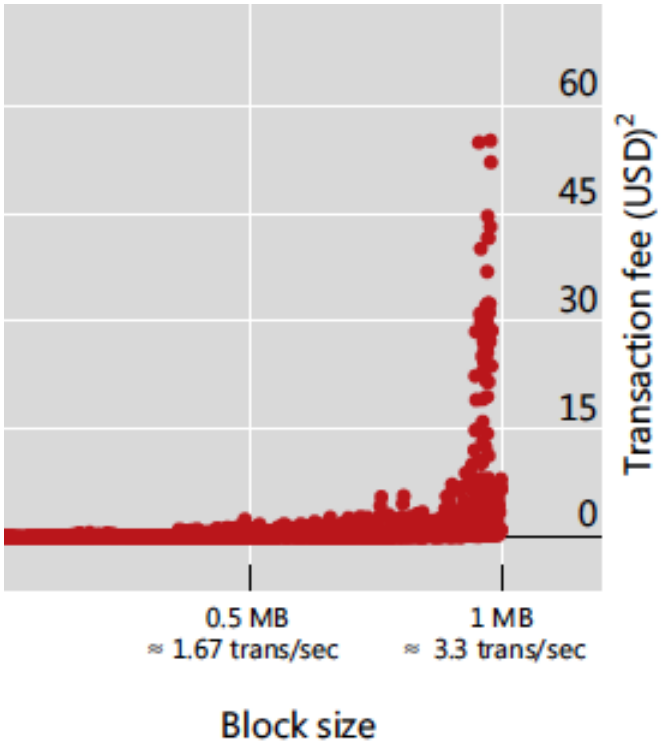

Abbildung 3: Zusammenhang zwischen Blockgrösse und Transaktionsgebühren (Auer (2019)).

so schwanken.

Der Transaktionsmarkt befindet sich in einem Trittbrettfahrerproblem. Es können nicht genügend hohe Transaktionsgebühren generiert werden, weil diese die Sicherheit zwar erhöhen würden, dieser Nutzen jedoch dem ganzen Netzwerk zugute kommt. Die zu zahlende Transaktionsgebühr wird hingegen jeder Transaktion und jedem Nutzer individuell verrechnet. Der Anreiz, sich mit der eigenen Transaktionsgebühr zu beteiligen, lässt sich also aus Sicht eines rationalen Individuums in Frage stellen. Stattdessen scheint es sinnvoller zu sein, auf die anderen Nutzer, deren Transaktionen im gleichen Block sind, zu hoffen und sich ohne eigenen Aufwand am Nutzen aus der generierten Sicherheit zu beteiligen. Die Sicherheit ist also abhängig vom gesamten Level an Transaktionsgebühren in einem Block und nicht nur von der Gebühr, die jeder einzelne Nutzer für seine Transaktion setzt. Dies führt zu einem klassischen Trittbrett-

fahrerproblem. Für die formale Analyse wird wieder von Ungleichung (1) ausgegangen und vereinfachende Annahmen getroffen. Transaktionsgebühren sind in diesem Fall die einzige Belohnungskomponente, es bestehen N ausstehende Transaktionen mit Volumen S und Nutzer sind ungeduldig in Bezug auf die Wartezeit für die Bestätigung der Transaktionen, verbunden mit Kosten µS pro zusätzlichen Block an Wartezeit. Ungleichung (1) lässt sich folgendermassen umschreiben:

$$\sum_{i=b}^{i=b+Waittime} \sum_{t\ in\ i} Fee_t > SN * \left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash} \frac{P_{USD}}{P_{USD}^{Attack}} - 1 \right)^{-1} \quad (3)$$

Nutzer können sich entweder auf eine gemeinsame Optimierung in Form einer Minimierung der gemeinsamen Gebühr und der Wartekosten einigen oder eine lediglich den eigenen Nutzen maximierende Gebühr wählen. Im ersten Fall wird die Summe aus der gemeinsamen Gebühr und der Wartekosten minimiert. Daraus ergibt sich eine optimale Gebühr $\overline{F}$:

$$\overline{F} = \ S \sqrt{\mu \left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash} \frac{P_{USD}}{P_{USD}^{Attack}} - 1 \right)^{-1}} \quad (4)$$

Optimal ist diese Gebühr jedoch nur in Bezug auf die Bedingung (1), unter welcher Angriffe nicht lohnenswert sind und stellt nicht das soziale Optimum dar. Die Höhe der Gebühr ist abhängig vom Transaktionsvolumen S, welches wiederum positiv von der Ungeduld µ der Nutzer und den Kosten für einen Angreifer abhängt. Wenn die Kosten eines Angriffs tief sind, müssen Nutzer umso mehr Gebühren bezahlen, damit ihre Transaktionen in den Block aufgenommen werden.

Im zweiten Fall werden die Transaktionsgebühren von jedem Nutzer individuell gesetzt. Dabei kommt eine Abweichung der Nutzer von einer gemeinsamen Gebühr zustande. Die Bedingung für die Wartezeit (*waittime*) sieht folgendermassen aus:

$$Waittime N\tilde{F} + (F_j - \tilde{F}) > SN * \left(\frac{Cost\ per\ rented\ hash}{Cost\ per\ hash} \frac{P_{USD}}{P_{USD}^{Attack}} - 1 \right)^{-1} \quad (5)$$

F_j bezeichnet die Gebühr, die Individuum j zahlt, $\tilde{F}$ die Gebühr aller anderen Individuen. Jedes Individuum minimiert seine eigenen Kosten (F_j und die Kosten aus der Wartezeit), woraus sich folgende Bedingung erster Ordnung ergibt:

$$\frac{\partial(F_j + \mu Waittime)}{\partial F_j} = 1 - \frac{\mu S}{N\tilde{F}} \quad (6)$$

Falls Individuum j ungeduldig ist (hohes μ) oder alle anderen Nutzer tiefe Gebühren setzen (tiefes $\tilde{F}$), sinken die Kosten bei einer Erhöhung von F_j. Wenn also $\mu S > N\tilde{F}$, setzt der Nutzer eine hohe Gebühr, um die Wartezeit auf ein Minimum von einem Block zu reduzieren. Im umgekehrten Fall wird eine Gebühr gesetzt, die minimal grösser als null ist. Es würde ein Anreiz bestehen, eine hohe Gebühr zu wählen, wenn alle anderen tiefe Gebühren setzen, um die Sicherheit der eigenen Zahlung zu erhöhen. Wenn alle anderen hingegen eine hohe Gebühr setzen, ist die Wartezeit bereits tief und die Sicherheit zukünftiger Blocks gross genug, so dass sich der Nutzer für eine sehr tiefe Gebühr entscheiden wird. Das Spiel ist symmetrisch und alle Nutzer gehen gleich vor. Im Gleichgewicht sieht die Gebühr folgendermassen aus:

$$F_j = \tilde{F} = \frac{\mu \mathrm{S}}{N}$$

Zwei Faktoren führen dazu, dass die Transaktionsgebühr in diesem dezentralen Gleichgewicht tiefer ist als die optimale Gebühr. Einerseits sinkt die Gebühr, je höher die Anzahl Transaktionen N ist. Typischerweise ist diese Zahl aufgrund der maximalen Blockgrösse hoch. Andererseits

fliesst die Ungeduld μ der Nutzer direkt in die Formel ein. Im optimalen Gleichgewicht hingegen ist es die Wurzel aus μ und somit grösser als im dezentralen Spiel[4]. Die tiefere Transaktionsgebühr im dezentralen Fall erhöht die Wartezeiten erheblich (Auer (2019)).

4.1.3 Stärken und Schwächen der Studie

Die Studie von Auer (2019) analysiert zwei wichtige Grenzen einer auf Proof-of-Work basierenden Kryptowährung: die hohen Kosten bei der Gewährleistung der Transaktionssicherheit und die Unfähigkeit des Transaktionsmarktes, genügend hohe Transaktionsgebühren zu generieren. Der Fokus liegt dabei auf Bitcoin. Dies ist plausibel, da Bitcoin die gängigste Kryptowährung ist, die auf Proof-of-Work basiert. Aspekte aus Nakamoto (2008) werden kritisch beurteilt und so definiert, dass eine ökonomische Analyse möglich ist. Dank der sogenannten Economic Finality werden einerseits die hohen Kosten, die für die Sicherheit der Transaktionen aufzuwenden sind, andererseits aber auch die Probleme in Bezug auf die Transaktionsgebühren dargelegt. Das Einbauen von formalen Gegebenheiten lässt also im Gegensatz zu Nakamoto (2008) eine fundierte ökonomische Analyse der Grenzen vom Proof-of-Work und darauf basierenden Kryptowährungen zu. Fragestellungen aus Nakamoto (2008) werden aus einer anderen Perspektive interpretiert.

Nakamoto (2008) untersucht die Chance eines erfolgreichen Angriffs, wohingegen Auer (2019) die Anreize von potenziellen Angreifern analysiert. Auf dieser Basis lassen sich die entsprechenden formalen Bedingungen aufstellen, unter denen ein Double-Spending-Angriff für einen Angreifer nicht lohnenswert ist.

Das Modell und die einzelnen Rechenschritte basieren jedoch auf einer Vielzahl von vereinfachenden Annahmen. Bei der Umschreibung von Ungleichung (1) in Ungleichung (2) wird beispielsweise angenommen, dass sich Nutzer an die Regel von Nakamoto (2008), die längste Kette als die Richtige anzunehmen, halten ($\Pi^{HF} = 0$). In der Vergangenheit ist diese

[4]Da μ zwischen 0 und 1 liegt, ist die Wurzel daraus grösser.

Regel aber in einigen Fällen missachtet worden (Auer (2019)). In einem solchen Fall ($\Pi^{HF} > 0$) wäre ein Angriff schwieriger, weil die Regel der längsten Kette von Nakamoto (2008) ignoriert werden würde. Der Anreiz für Double-Spending wäre in diesem Szenario tiefer. Dies wiederum hätte einen Einfluss auf die Kosten der dezentralen Gewährleistung der Transaktionssicherheit: Wenn Double-Spending weniger lohnenswert ist, sind die Kosten, dies zu verhindern, gemäss dem Modell von Auer (2019) entsprechend tiefer. Aus diesem Grund ist die Annahme von $\Pi^{HF} = 0$ an dieser Stelle sehr zweifelhaft. Die Aussagekraft und Korrektheit dieses Modells ist deshalb zu hinterfragen.

Diese Zusammenhänge verdeutlichen die Wichtigkeit der getroffenen Annahmen. Eine weitere kritische Annahme stellt dar, dass zu jedem Zeitpunkt eine beliebige Menge an Mining-Ressourcen beschafft werden kann. Dies betrifft den Fall, in dem ein Angreifer kurzfristig Mining-Ressourcen benötigt, um einen Angriff starten zu können. Aufgrund des gesunkenen Bitcoin-Preises können viele Miner ihre Stromkosten nicht mehr decken. In einem solchen Szenario scheint es jedoch plausibel zu sein, die Rechner kurzfristig wieder einzuschalten, sobald sich die Möglichkeit für einen rentablen Double-Spending-Angriff ergibt (Auer (2019)). Im Vergleich zu der Zeit, in der der Bitcoin-Preis höher war, scheint ein Angriff auf Bitcoin aktuell also realistischer zu sein. Auer (2019) betont anhand dieser Zusammenhänge, dass sich in nächster Zeit immer mehr Mining-Ressourcen vom regulären Markt in den Angriffsmarkt verschieben werden. Doch wie realistisch ist die Annahme, dass zu jedem Zeitpunkt Mining-Ressourcen beschafft werden können? Laut Xie (2019) ist die Mehrheit der global existierenden Rechenleistung illiquide und somit nicht verfügbar. Deshalb kann diese Annahme von Auer (2019) ebenfalls als kritisch bewertet werden.

Auer (2019) kombiniert insgesamt wichtige Faktoren wie Transaktionsgebühren, Double-Spending Anreize und die Sicherheit des Systems, um die ökonomischen Grenzen von Bitcoin aufzuzeigen. Andere Studien gehen beispielsweise von einer Stauung (*congestion*) im Transaktionsmarkt aus (Huberman et al. (2017)), was beim Erreichen der maximalen Block-

grösse geschehen kann und zu höheren Transaktionsgebühren führt. Budish (2018) untersucht ebenfalls die ökonomische Bedeutung von Double-Spending in Bezug auf die Sicherheit des Systems, die genaue Bestimmung des Mining-Einkomens jedoch nicht. In Auer (2019) werden diese Faktoren kombiniert untersucht, was eine Stärke der Studie ist. Anhand der Gegebenheiten im Transaktionsmarkt wird die Sicherheit der Zahlungen im Bitcoin-System analysiert und auf dieser Basis zukünftige Entwicklungen interpretiert. Obwohl die Studie ökonomisch ausgerichtet ist, werden auch technische Grundlagen über Bitcoin und die Blockchain erklärt.

Die Studie besagt anhand des Problems der zu tiefen Transaktionsgebühren und der periodisch halbierten Coin Rewards, dass die Bitcoin-Liquidität sinken wird. Doch wenn davon ausgegangen wird, dass aufgrund dieser Grenzen Coin Rewards einmal wegfallen werden, wird nicht die Liquidität, sondern die Bitcoinmenge darunter leiden. Es wird kein plausibler Zusammenhang mit der Liquidität beschrieben. Plausibler wäre, dass nach dem Wegfallen der Coin Rewards der Anreiz für Mining sinken wird, wenn die Transaktionsgebühren nicht entsprechend erhöht werden können. Somit würde die Bitcoin-Schöpfung und die Wachstumsrate der Bitcoinmenge verlangsamen. Berentsen und Schär (2017) erwähnen unter anderem auch, dass die Belohnung in Form von neuen Bitcoins die Geldmenge ausdehnt. Wenn diese Belohnung also wegfällt, würde die Bitcoinmenge zurückgehen. Berentsen und Schär (2017) zeigen ausserdem den rückläufigen Wachstumsprozess der Anzahl Bitcoins auf. Nebst den periodisch halbierten Coin Rewards wird der Rückgang darauf zurückgeführt, «dass eine stetig zunehmende monetäre Basis, relativ gesehen, zu geringeren Wachstumsraten führt» (Berentsen und Schär (2017, S. 256/257)).

Weiter zieht Auer (2019) bezüglich der sinkenden Coin Rewards den Schluss, dass die Bestätigung der Transaktionen sehr lange dauern kann. Im Bitcoin-Netzwerk ist aber das Intervall, mit dem neue Blocks erstellt werden, mittels einem Schwellenwert und der sich daraus ergebenden *Difficulty* geregelt. Der Schwellenwert wird jeweils so angepasst, dass der

zehn Minuten Schnitt erhalten bleibt. Die Difficulty steht dabei in einem gegensätzlichen Verhältnis zum Schwellenwert. Je höher dieser ist, umso einfacher wird ein gültiger Block gefunden. Eine Anpassung des Schwellenwertes findet jeweils nach genau 2'016 neu erstellten gültigen Blocks statt. Bei einem zehn Minuten Schnitt würde eine Periode also 20'160 Minuten respektive zwei Wochen dauern. Die Anpassung des Schwellenwertes δ findet auf Basis dieses Erwartungswertes $E(t)$ und der tatsächlichen Zeitdauer t statt. Der neue Schwellenwert wird folgendermassen berechnet (Berentsen und Schär (2017, S. 211)):

$$\delta_{neu} = \delta_{alt} \ \frac{t}{E(t)} = \delta_{alt} \ \frac{t}{20160}$$

Falls die tatsächliche Zeit tiefer ist als im Erwartungswert, wird der neue Schwellenwert also tiefer sein. Dies erhöht die Difficulty und bringt den Schnitt wieder in die Nähe des zehn Minuten Schnitts. Im umgekehrten Fall wird der zweite Faktor der Gleichung über 1 liegen, der neue Schwellenwert höher sein als der alte und die Difficulty folglich sinken. Die Difficulty-Schwellenwert-Relation sieht folgendermassen aus (Berentsen und Schär (2017, S. 212)):

$$D_i = \frac{1/\delta(B_i)}{1/\delta(B_0)} = \frac{\delta(B_0)}{\delta(B_i)}$$

Dies entspricht dem Kehrwert des maximalen Schwellenwertes $\delta(B_0)$ geteilt durch den Kehrwert des aktuellen Schwellenwertes $\delta(B_i)$. Der Schwellenwert muss angepasst werden, weil die Rechenleistung kontinuierlich zunimmt und das Finden gültiger Blocks schneller geschieht (Berentsen und Schär (2017)). Nur durch eine regelmässige Senkung des Schwellenwertes kann also der zehn Minuten Schnitt erhalten bleiben. In der Studie von Auer (2019) werden diese Aspekte nicht berücksichtigt. Die Aussage, dass Transaktionsbestätigungen sehr lange dauern werden, sobald die Coin Rewards wegfallen, kann unter Berücksichtigung des Schwellenwer-

tes und der Difficulty somit als fragwürdig bewertet werden.

Eine Konklusion von Auer (2019), die für die Zukunft bedeutend sein könnte, ist, dass das System nicht komplett dezentral aufgebaut sein muss, sondern Institutionen in Problemfällen lenkend eingreifen können. So könnten laut Auer (2019) zum Beispiel Probleme in der Konsensfindung, die dezentral nicht überwunden werden können, über zentrale Instanzen behoben werden. Eine wichtige Erkenntnis für die Zukunft könnte zudem lauten, dass die Technologie traditionelle Zahlungssysteme nicht komplett verdrängen, sondern bestehende Systeme verbessern soll. Mögliche Zukunftsentwicklungen werden von Auer (2019) gut adressiert, um den Forschungsbedarf zu verdeutlichen. Trotz einigen Kontroversen und Behauptungen über Probleme geht die Studie auf Second-Layer Lösungen ein. Behandelte Problemzonen werden also nicht stehen gelassen. Anhand der aktuellen Entwicklungen wird ein guter Ausblick für die Lösung bestimmter Probleme ermöglicht. Dabei wird vorwiegend auf das Lightning-Netzwerk eingegangen.

Solche dezentralen Zahlungsnetzwerke ermöglichen Zahlungen zwischen beliebigen Nutzern abseits der Blockchain, sofern Absender und Empfänger über einen oder mehrere Zahlungskanäle verbunden sind. Zunächst muss aber ein Pre-Funding[5] stattfinden, damit die Teilnehmer weitere Transaktionen durchführen können. Nach dem der benötigte Betrag durch Pre-Funding Transaktionen erreicht ist, sind die Teilnehmer in der Lage, die eigentlichen Zahlungen untereinander auszutauschen (Auer (2019)). In der Studie wird jedoch hinterfragt, ob ein Teilnehmer dazu bereit wäre, solche Pre-Funding Beträge auf sich zu nehmen, um das Funktionieren des Systems zu unterstützen. Ein Nachteil des Lightning

[5]Wenn eine Zahlung mehrere Zwischenkanäle durchläuft, ist dementsprechend eine höhere Vorfinanzierung nötig, um die benötigte Kapazität für die Kanäle zu gewährleisten. Bei vier Zwischenkanälen wäre ein um das fünffache höherer Finanzierungsbetrag nötig als der Betrag der eigentlichen Zahlung (Auer (2019)). Ausserdem werden für einen sicheren Transfer in einem Zahlungskanal Smart Contracts benötigt. Im Rahmen sogenannter *Hashed Timelock Contracts* muss der Empfänger innerhalb einer festgelegten Zeit den Erhalt einer Zahlung durch einen kryptografischen Zahlungsnachweis bestätigen. Ansonsten verfällt der Anspruch auf die Zahlung. Durch solche Smart Contracts kann das Gegenparteirisiko eliminiert werden (Poon und Dryja (2016)).

Netzwerkes ist zudem, dass Stand Anfang Januar 2019 rund zwei Drittel der Transaktionen über einen einzigen Anbieter stattgefunden haben, was nicht im Sinne der angestrebten Dezentralisierung ist (Auer (2019)). Als Vorteil gelten hingegen die erhöhte Skalierbarkeit und die kürzere Wartezeit (Berentsen und Schär (2017)). Weil die einzelnen Zahlungen abseits der Blockchain stattfinden und nur der Abschluss von Zahlungskanälen über die Blockchain geschieht, wird die Blockchain entlastet (Auer (2019)). Ein Anwendungsbeispiel stellen dabei Atomic Swaps dar, auf die in Kapitel 3.4 dieser Arbeit eingegangen wurde. Auch wenn diese Lösungsansätze noch in Entwicklung sind und einige Nachteile aufweisen, wird deren Bedeutung ersichtlich, da bereits viele Studien Second-Layer Lösungen thematisieren.

4.2 Bitcoin Microstructure and the Kimchi Premium (Choi et al. (2018))

Die Studie von Choi et al. (2018) wurde herangezogen, weil sie die Preisunterschiede von Bitcoin und anderen Kryptowährungen sehr gut aufzeigt. Der Vergleich zwischen verschiedenen Ländern mit unterschiedlichen regierungsspezifischen Gegebenheiten sowie der Vergleich der Bitcoin-Prämie mit derjenigen anderer Kryptowährungen liefert interessante Erkenntnisse.

4.2.1 Idee der Studie

Diese Studie untersucht Mechanismen und Zusammenhänge, die zu Preisunterschieden in Bitcoin führen. Der Vergleich zwischen dem südkoreanischen und US-amerikanischen Markt steht dabei im Vordergrund. Der Preisunterschied in Bitcoin zwischen diesen Märkten wird als Kimchi-Prämie bezeichnet. Gründe für die höheren Bitcoin-Preise in bestimmten Ländern – wie beispielsweise in Südkorea – werden anhand der Mikrostruktur von Bitcoin diskutiert. Nebst der Mikrostruktur ist auch der Kapitalverkehr verantwortlich für Preisunterschiede. Choi et al. (2018)

zeigen, dass Länder mit restriktivem Kapitalverkehr höhere Prämien aufweisen. Allgemein ausgedrückt ist die ökonomische Freiheit eines Landes entscheidend in Bezug auf den Bitcoin-Preis in diesem Land. Ein restriktiverer Kapitalverkehr erhöht laut Choi et al. (2018) auch den Effekt der Mikrostruktur auf die Prämien. Das gilt auch für Südkorea, wo die Kimchi-Prämie aufgrund des restriktiveren Kapitalverkehrs sensibler auf mikrostrukturelle Faktoren wie Transaktionskosten, Bestätigungszeiten und Volatilitäten reagiert. Das bedeutet, dass die Kimchi-Prämie - im Vergleich zur Prämie eines anderen Landes mit einer höheren ökonomischen Freiheit - einen höheren Anstieg verzeichnet, wenn sich diese Mikrostruktureffekte verstärken. Ein internationaler Vergleich der Bitcoin-Prämien, wobei Mikrostruktureffekte isoliert werden, zeigt den direkten Zusammenhang zwischen der ökonomischen Freiheit und tieferen Prämien. In Bezug auf Mikrostruktureffekte werden Faktoren analysiert, die Arbitrage Anreize reduzieren. Höhere Transaktionsgebühren, Volatilitäten und längere Bestätigungszeiten erschweren Arbitrage, wodurch es zu Preisunterschieden kommt. Ein weiterer wichtiger Faktor ist das Handelsvolumen. Entgegen der Literatur über die Blasenbildung an den Börsen besagen Choi et al. (2018), dass ein hohes Handelsvolumen die Kimchi-Prämie reduziert. Laut dieser Studie ist die Erhöhung der Liquidität durch ein höheres Handelsvolumen grösser als die Erhöhung der Transaktionsgebühren, wodurch der positive Effekt überwiegt und die Kimchi-Prämie insgesamt sinkt. Diese Schlussfolgerungen ergeben sich erst durch den Vergleich des südkoreanischen und europäischen Marktes und in einem zweiten Schritt durch eine internationale Analyse.

4.2.2 Analyse des Modells

Anhand einer ersten Regression werden Unterschiede im Bitcoin-Preis zwischen Südkorea und den USA gemessen. Dabei werden verschiedene erklärende Variablen festgelegt und deren Effekt auf die Kimchi-Prämie berechnet. Diese stellt den Preisunterschied beim Kauf von Bitcoin mit südkoreanischen Won gegenüber US-Dollar dar und sieht folgendermassen aus:

$$\text{Kimchi-Prämie} = \frac{\text{KRWBTCprice in USD}}{\text{USDBTCprice}} - 1$$

In der ersten Regression kommen sieben erklärende Variablen vor. Die erste Variable, die kurzfristige Bitcoin-Volatilität, weist einen signifikant positiven Zusammenhang zur Kimchi-Prämie auf. Dies lässt sich mit gesunkenen Arbitrage-Anreizen – ausgelöst durch die höheren Wartekosten für die Transaktionsbestätigung bei einer hohen Volatilität – erklären. Die preisausgleichende Funktion der Arbitrage fällt weg, was Preisdifferenzen begünstigt. Die zweite Variable, die Transaktionsgebühren, haben einen ähnlichen Effekt auf die Kimchi-Prämie. Längere Bestätigungszeiten führen ebenfalls zu signifikant höheren Prämien. Die Möglichkeit für einen Arbitrageur, dies mit einer höheren Transaktionsgebühr zu umgehen, erscheint aufgrund des gerade erwähnten positiven Zusammenhangs mit der Kimchi-Prämie nicht plausibel. Der alleinige Effekt eines höheren Handelsvolumens auf die Kimchi-Prämie ist positiv.

Wenn jedoch alle bisherigen erklärenden Variablen gemeinsam in einer Regression analysiert werden, stellt sich heraus, dass das Handelsvolumen einen signifikant negativen, die kurzfristige Bitcoin-Volatilität sowie Transaktionsgebühren hingegen einen signifikant positiven Einfluss auf die Höhe der Kimchi-Prämie aufweisen. Der Median der Bestätigungszeit sowie der Wechselkurs zwischen dem südkoreanischen Won und dem US-Dollar haben in der gemeinsamen Analyse keinen signifikanten Effekt auf die Kimchi-Prämie. Bitcoin-Returns stehen wiederum in einer signifikant positiven Relation zur Kimchi-Prämie. Nachrichten über Bitcoin in Südkorea haben ebenfalls einen signifikanten Effekt. Da überwiegend negative News erscheinen, hat diese Variable einen signifikant negativen Einfluss auf die Kimchi-Prämie (Prämie sinkt). Im umgekehrten Szenario würde die Prämie hingegen tendenziell steigen.

Um den Effekt von Kapitalverkehrskontrollen in Südkorea auf die Kimchi-Prämie messen zu können, wird in einer zweiten Regression der europäische Markt untersucht. Die Prämie beschreibt die Differenz beim Kauf

von Bitcoin mit Euros und US-Dollar und wird wie folgt berechnet:

$$\text{Prämie} = \frac{\text{EURBTCprice in USD}}{\text{USDBTCprice}} - 1$$

Die kurzfristige Bitcoin-Volatilität, Transaktionsgebühren und die Bestätigungszeiten haben erneut einen positiven Einfluss auf die Bitcoin-Prämie, der absolute Effekt ist aber jeweils um ein Vielfaches kleiner als im südkoreanischen Markt. Die Mikrostruktur von Bitcoin hat somit einen Anteil an den Preisdifferenzen. Es gilt aber zu beachten, dass die Prämie im europäischen Markt fast null, im südkoreanischen Markt hingegen deutlich positiv ist. Dieses Resultat weist auf die Existenz eines Faktors hin, der diesen Unterschied erklärt (Choi et al. (2018)).

Choi et al. (2018) untersuchen deshalb den Aspekt der ökonomischen Freiheit. In einer internationalen Analyse wird gezeigt, wie die Bitcoin-Prämie von der Offenheit der Finanzmärkte abhängt. Dabei wird der Bitcoin-Preis im jeweiligen Land in US-Dollar umgerechnet (LCBTCprice in USD). Die Prämie stellt die prozentuale Abweichung vom Bitcoin-Preis in den USA (USDBTCprice) dar und sieht folgendermassen aus:

$$\text{Prämie} = \frac{\text{LCBTCprice in USD}}{\text{USDBTCprice}} - 1$$

In der Regressionsanalyse stellt diese Prämie die abhängige Variable dar. Die ökonomische Freiheit ist eine der erklärenden Variablen. Diese setzt sich aus verschiedensten Faktoren zusammen. Choi et al. (2018) lehnen sich dabei an das Fraser Institute (2019), das die einzelnen Variablen in fünf Gruppen kategorisieren: (1) die Grösse der Regierung, (2) das Rechtssystem und die Sicherheit bezüglich Eigentumsrechte, (3) stabiles Geld (*sound money*), (4) Regulierung, (5) Grad der Freiheit für internationalen Handel. Laut dem Fraser Institute (2019) beinhalten die fünf Kategorien folgende Faktoren, die hier aufgelistet werden, um die Bedeu-

tung der Kategorien zu verdeutlichen:

1. Grösse der Regierung:

   - Staatliche Konsumausgaben
   - Transfers und Subventionen
   - Staatliche Unternehmen und Investitionen
   - Maximaler Grenzsteuersatz

2. Rechtssystem und Eigentumsrechte:

   - Unabhängigkeit der Justiz
   - Unparteilichkeit der Gerichte
   - Schutz der Eigentumsrechte
   - Präsenz des Militärs in Sachen Rechtsstaatlichkeit und Politik
   - Integrität des Rechtssystems
   - Rechtliche Durchsetzung von Verträgen
   - Regulierungskosten für den Verkauf von Immobilien
   - Zuverlässigkeit der Polizei
   - Kosten der Kriminalität

3. Stabilität des Geldes:

   - Geldmengenwachstum
   - Standardabweichung der Inflation
   - Inflation im vergangenen Jahr

- Die Freiheit, Fremdwährung zu besitzen

4. Regulierung:

- Regulierung im Kreditmarkt
- Regulierung im Arbeitsmarkt
- Geschäftsbestimmungen (*Business regulations*)

5. Freiheit für internationalen Handel:

- Zölle
- Regulatorische Handelshemmnisse
- Wechselkurse am Schwarzmarkt
- Kapital- und Personenverkehrskontrollen

Diese Faktoren werden für jedes Land auf einer Skala von 1 bis 10 bewertet, der Durchschnitt aller fünf Kategorien gebildet und so der Grad der ökonomischen Freiheit bestimmt. Die Regression bestätigt das erwartete Resultat. Die ökonomische Freiheit korreliert negativ mit der Bitcoin-Prämie. Länder mit einer höheren ökonomischen Freiheit weisen signifikant tiefere Prämien auf. Auch die Variable für Kapitalverkehrskontrollen impliziert denselben Zusammenhang. In Ländern, in denen Kapitalverkehrskontrollen strenger sind, resultiert eine signifikant höhere Bitcoin-Prämie. Somit sind Länder, in denen der Eingriff in die Finanzmärkte stärker und restriktiver ist, eher einer hohen Bitcoin-Prämie ausgesetzt. Die bei der Analyse des südkoreanischen Marktes gewonnenen Erkenntnisse lassen sich ebenfalls wiederfinden. Längere Bestätigungszeiten, höhere Transaktionsgebühren sowie Volatilitäten erschweren Arbitrage und lösen höhere Prämien aus (Choi et al. (2018)).

Nach diesen Schlussfolgerungen kann die Frage gestellt werden, wie die Prämien für andere Kryptowährungen wie beispielsweise Ethereum oder

Ripple aussehen. Die Autoren stellen fest, dass die Ethereum-, Ripple- und Litecoin-Prämien in Südkorea von der Bitcoin-Prämie kaum zu unterscheiden sind. Auch die Standardabweichungen sind sehr ähnlich. Arbitrage zwischen Kryptowährungen wäre im Fall von Südkorea theoretisch möglich, denn Kapitalverkehrskontrollen gelten lediglich für Fiatgeld. Aufgrund der vernachlässigbar kleinen Unterschiede in den Prämien lohnt sich Arbitrage aber nicht und die Transaktionskosten sind im Vergleich dazu zu hoch. Die Korrelationen zwischen der Kimchi-Prämie und den jeweils restlichen drei Prämien wie auch die paarweisen Korrelationen liegen zwischen knapp 0.9 und 1 (Choi et al. (2018)).

Diese Fakten gehen mit den Aussagen der Autoren bezüglich der Kapitalverkehrskontrollen und der Kimchi-Prämie einher. Kapitalverkehrskontrollen führen dazu, dass Arbitrage zwischen den Märkten für Kryptowährungen erschwert wird. Dies wiederum führt zu positiven Prämien für die jeweilige Kryptowährung, woraus sehr ähnliche Prämien abgeleitet werden können. Sehr ähnliche Prämien reduzieren Arbitrageanreize zwischen den Kryptowährungen selber. Choi et al. (2018) stellen somit fest, dass die Kimchi-Prämie kein Bitcoin eigenes Phänomen ist. Der treibende Faktor bleibt die Offenheit der Ökonomie und der Finanzmärkte, was am Beispiel Südkorea mit strengen Kapitalverkehrskontrollen deutlich wird.

4.2.3 Stärken und Schwächen der Studie

Die Studie von Choi et al. (2018) untersucht die verschiedenen Gründe für internationale Preisdifferenzen. Die Analyse richtet sich an den südkoreanischen Bitcoin-Markt, der mit dem europäischen und US-amerikanischen Markt verglichen wird. Die höheren Prämien in Südkorea deuten darauf hin, dass die Bitcoin-Mikrostruktur nicht die einzige Komponente sein kann, die Einfluss auf Bitcoin-Prämien nimmt. Diese Erkenntnis führt zur eigentlichen Analyse über den Faktor der ökonomischen Freiheit. Dieser erweist sich als entscheidend für die höheren Prämien in Südkorea. Die Vorgehensweise von Choi et al. (2018) zeigt deutlich, dass Regierungen

eine entscheidende Rolle bei der Preisbildung von Kryptowährungen spielen können. Die Methodik in dieser Studie scheint also sinnvoll zu sein und ebnet den Weg zu dieser neuen Erkenntnis. Folglich können über die südkoreanischen Grenzen hinaus andere Länder mit unterschiedlicher ökonomischer Freiheit untersucht werden, was einen guten Beitrag zur Forschung rund um das Thema Prämien und Bitcoin-Mikrostruktur leistet.

Eine weitere sinnvolle Analyse stellt der Vergleich von Bitcoin mit anderen Kryptowährungen dar. Aus der Sicht von (potenziellen) Investoren kann es wichtig sein zu wissen, ob die oben erwähnten Phänomene Bitcoin eigen sind. Choi et al. (2018) zeigen, dass dem nicht so ist. Die Wahl des Regressionsmodells und Erläuterungen zur untersuchten Stichprobe wurden detailliert beschrieben und begründet. Die Ergebnisse der ersten Regression, bei der die Determinanten der Kimchi-Prämie untersucht werden, sind hochsignifikant (99% Konfidenzniveau). In der zweiten Regression zu den Preisunterschieden zwischen Europa und den USA sind die Ergebnisse mindestens für ein 95% Konfidenzniveau signifikant, wobei die unabhängigen Variablen in der ersten Regression einen deutlich höheren Anteil an der Varianz der abhängigen Variablen erklären. Weshalb das Bestimmtheitsmass R^2 in den beiden Regressionen so stark variiert, wird von Choi et al. (2018) nicht erklärt, wäre für die Interpretation der Resultate aber von Interesse.

Obwohl der Zeithorizont der herangezogenen Daten für die Regressionen kurz ist (01.01.2016-28.02.2018), gibt es mit rund 13 Millionen Transaktionen relativ viele Observationen. Die Wahl des Zeithorizontes ist sinnvoll, weil die Preisunterschiede davor vernachlässigbar waren (Oh (2018)). Die Daten wurden unter der Verwendung verschiedenster Handelsplattformen zusammengestellt, was die Anzahl an verfügbaren Daten erhöht und somit mehr Informationen einbringt. Insgesamt wird die Zusammensetzung der Daten detailliert begründet und Formeln für die Berechnung der abhängigen Variablen erläutert.

Ausserdem führen Choi et al. (2018) einige Robustheitstests durch. Die für die Regression verwendete kurzfristige Bitcoin-Volatilität wird durch

eine zusätzliche Berechnung der langfristigen Volatilität ergänzt, was robuste Resultate liefert. Tage ohne Handelsdaten werden ausgeschlossen. Mittels linearer Interpolation zwischen den fehlenden Handelstagen wird ein weiterer Robustheitstest durchgeführt und ebenfalls robuste Resultate erzielt. Beim Vergleich der Kimchi-Prämie mit derjenigen anderer Kryptowährungen werden die Handelsplattformen Bithumb (für Südkorea) und Kraken (für USA) verwendet. Aufgrund eines Handelsstopps auf Kraken schliessen Choi et al. (2018) drei Handelstage aus. Durch Ersetzen der fehlenden drei Handelstage durch Daten aus der Plattform Bitstamp wird die Robustheit der Resultate bestätigt. Dies erhöht die Zuverlässigkeit der Resultate aus den Regressionen.

Die Ergebnisse der Studie liefern einen wichtigen Beitrag zur Forschung. Die Studie kommt zum Schluss, dass das Handelsvolumen – entgegen der Literatur zur Blasenbildung an den Börsen – negativ mit der Kimchi-Prämie zusammenhängt. Eine weitere Vergleichsgrösse stellt die Zukunft von dezentralen Zahlungssystemen dar. Ähnlich wie in der ersten untersuchten Studie von Auer (2019) stellen auch Choi et al. (2018) fest, dass ein rein dezentrales Zahlungssystem ohne zentrale Koordinationsmechanismen eine unrealistische Zukunftserwartung ist. Zu erwähnen gilt es jedoch, dass dies dem Urgedanken von Nakamoto (2008) bezüglich eines rein dezentralen Zahlungssystems widerspricht. Unter Berücksichtigung von Second-Layer Lösungen ist es aus Sicht des Autors der vorliegenden Arbeit durchaus möglich, die Obergrenze der Kapazität des Bitcoin-Systems mit Hilfe von Off-Blockchain Transaktionen zu erhöhen, ohne dabei vom Urgedanken von Nakamoto (2008) abzuweichen.

Der Ausblick der Studie von Choi et al. (2018) ist auf die Aussage über die Zukunft eines rein dezentralen Zahlungssystems beschränkt und erschwert die Möglichkeit, aufgrund der Erkenntnisse zukünftige Entwicklungen in Bezug auf Preisdifferenzen abzuschätzen. Anhand der aufgezeigten Probleme und Grenzen sind jedoch zukünftige Forschungsschwerpunkte zu erkennen. Die Grenzen der Kryptowährungen werden wie in Auer (2019) und Choi et al. (2018) oft auf die Mikrostruktur zurückgeführt. Gleichzeitig werden aber auch Einflüsse externer Faktoren wie Re-

gulierung, Koordination und Regierungen sowie länderspezifische Aspekte unter die Lupe genommen, um ökonomische Probleme zu begründen. Die detaillierte länderspezifische Analyse der Bitcoin-Prämien in Choi et al. (2018) schafft neue, für zukünftige Studien interessante Erkenntnisse.

Zwei Aspekte fallen bei der Analyse weiterer Studien zu diesem Thema jedoch auf. Erstens wird die mittlerweile wieder zurückgegangene Kimchi-Prämie von Choi et al. (2018) nicht angesprochen. Yim et al. (2018) berichten, dass die Prämie zeitweise sogar eine inverse Form angenommen hat und Preise in Südkorea tiefer waren. Zweitens liefert die Literatur – nebst den Kapitalverkehrskontrollen – weitere Gründe für den Anstieg der Preisdifferenzen zwischen Südkorea und ausländischen Märkten. Genauer ausgedrückt macht Oh (2018) drei andere Faktoren direkt für die Kimchi-Prämie verantwortlich, wobei Kapitalverkehrskontrollen als Grund für das Misslingen der Eliminierung der Preisunterschiede durch Arbitrage bezeichnet werden. Die drei Determinanten der Kimchi-Prämie sind Unterschiede in den Returns der Kryptowährung, die Zinssätze der Landeswährungen und die erwarteten Wechselkurse der Kryptowährung in Südkorea und den USA. Oh (2018) studiert somit auch makroökonomische Determinanten. In Choi et al. (2018) gehen zwar makroökonomische Aspekte in das Modell ein, jedoch indirekt über den Faktor der ökonomischen Freiheit, welcher als Hauptursache für die Kimchi-Prämie dargestellt wird.

Die Kimchi-Prämie begann erst ab Ende 2017 zu steigen und die Preisdifferenzen zwischen Südkorea und den USA erreichten Anfang 2018 den Höhepunkt (Oh (2018)). Der anschliessende Rückgang wird auf die Bemühungen der südkoreanischen Regierung, die Prämie zu senken, zurückgeführt. Zuvor war die südkoreanische Regierung gegenüber Kryptowährungen skeptisch, obwohl Südkorea zu dieser Zeit mit einem Anteil von rund 15% am gesamten Handel einer der führenden Märkte für Kryptowährungen war. Die Kimchi-Prämie ist in der Zwischenzeit gesunken, obwohl die Regulierungen im Markt für Kryptowährungen durch die Regierung zugenommen haben. Dies deutet darauf hin, dass wie erwar-

tet andere Faktoren Einfluss auf die Kimchi-Prämie nehmen und diese nicht nur über die ökonomische Freiheit zu erklären ist. Aus der Analyse geht hervor, dass die Kimchi-Prämie den drei genannten Determinanten geschuldet ist. Faktoren wie beispielsweise Regulierung, Liquidität oder Handelsvolumen können die Prämie aber ebenfalls beeinflussen. Dabei stehen folgende vier Kategorien in einer Wechselwirkung zueinander und beeinflussen gemeinsam die Preise: Die Blockchain-Technologie, der Kryptomarkt, ökonomische Variablen und Regulierung (Oh (2018)).

Die Studie von Oh (2018) bietet insgesamt eine breitere Analyse der Determinanten der Kimchi-Prämie. Schlussfolgerungen aus der Studie von Choi et al. (2018) lassen sich aus einer neuen Perspektive beurteilen. Daraus lässt sich schliessen, dass Preisdifferenzen ein facettenreicheres Phänomen darstellen und nicht nur durch die ökonomische Freiheit erklärt werden können. Der Vorteil der letzteren Studie ist wiederum, dass sie mit Daten arbeitet und ihre Ergebnisse auf statistischen Tests basieren. Ansätze von Oh (2018) wurden empirisch noch nicht belegt, was Gegenstand weiterer Studien bezüglich dieser Thematik sein könnte.

Wie sieht der aktuelle Stand aus? Der Vergleich der Bitcoinpreise an südkoreanischen und US-amerikanischen Exchanges liefert sehr ähnliche Preise. Stand 18. Dezember 2019 wird Bitcoin beispielsweise auf der US-amerikanischen Plattform Coinbase (2019) für knapp 6'700 US-Dollar gehandelt, an der südkoreanischen Exchange Bithumb (2019) hingegen umgerechnet für knapp 6'800 US-Dollar. An dieser Stelle soll die Kimchi-Prämie allerdings nicht neu berechnet, sondern lediglich die Annährung der Preise im Vergleich zur Phase mit sehr grossen Preisdifferenzen aufgezeigt werden. Insgesamt liefert die Studie von Choi et al. (2018) wichtige Erkenntnisse zum Thema Preisdifferenzen. Andere Studien zu dieser Thematik - wie Oh (2018) - identifizieren aber ebenso interessante und von Choi et al. (2018) nicht erwähnte Determinanten der Preisdifferenzen für Kryptowährungen.

4.3 Abschliessende Bemerkungen

Die Detailanalyse liefert einerseits einen Überblick über ökonomische Eigenschaften der Blockchain und Kryptowährungen und zeigt mögliche ökonomische Probleme und Grenzen im Detail auf. Andererseits bietet die Analyse aber auch Raum für Diskussionen, wie legitim und sinnvoll die Schlussfolgerungen der jeweiligen Studien sind. Wie dieses Kapitel gezeigt hat, lassen sich viele Aspekte in der Literatur hinterfragen. In der folgenden Diskussion werden die wichtigsten Erkenntnisse zusammengefasst. Anhand der untersuchten Studien wird der aktuelle Stand der ökonomischen Literatur zu Blockchain und Kryptowährungen generell bewertet und auf mögliche Zukunftsentwicklungen eingegangen.

5 Diskussion

Die in dieser Arbeit behandelte ökonomische Literatur über die Blockchain und Kryptowährungen diskutiert viele verschiedene Aspekte. Die grundsätzliche Erkenntnis ist, dass die bestehende Literatur mit Vorsicht zu geniessen ist.

Für die Gewährleistung der Mining-Anreize und der damit zusammenhängenden Transaktionssicherheit spielen die Transaktionsgebühren eine entscheidende Rolle. Diese Wichtigkeit wird von Chiu und Koeppl (2017) missachtet. Wie auch Berentsen und Schär (2017) betonen, steigt die Bedeutung der Transaktionsgebühren angesichts der periodisch halbierten Coin Rewards sogar immer weiter. Der Anteil der Transaktionsgebühren an der gesamten Belohnung sollte erhöht werden, um die Anreize der Miner, neue Transaktionen in ihre Blocks aufzunehmen, sicherzustellen (Berentsen und Schär (2017)). Transaktionsgebühren werden zudem für die Verhinderung von DDoS Angriffen benötigt, wie am Beispiel von Mempool Angriffen und dem Fee-based Ansatz gezeigt wurde. Dabei werden nur Transaktionen akzeptiert, die auch mit der Absicht initiiert wurden, in die Blockchain aufgenommen zu werden. Transaktionen im Rahmen eines Angriffs werden aussortiert. Dazu muss ein Initiant nicht nur für

die Mining-Gebühr aufkommen, sondern auch für die minimale Gebühr für die Weiterleitung der Transaktion an die anderen Knoten (minimum relay fee). Transaktionen, die für diese Gebühren nicht aufkommen, werden abgelehnt (Saad et al. (2018)). Aufgrund dieser Argumente kann die Aussage von Chiu und Koeppl (2017), dass die Belohnung der Miner ausschliesslich durch neu geschöpfte Coins finanziert werden sollte, kritisiert werden.

Ähnlich wie Chiu und Koeppl (2017) befasst sich Auer (2019) mit den beiden Belohnungskomponenten der Miner. Der Unterschied zwischen diesen Studien ist allerdings, dass Auer (2019) auf die Wichtigkeit der Transaktionsgebühren aufmerksam macht, während Chiu und Koeppl (2017) eine ausschliessliche Finanzierung der Belohnung durch neu geschöpfte Coins vorschlagen. Die Schlussfolgerung von Auer (2019) ist wiederum insofern zweifelhaft, dass eine starke Erhöhung der Bestätigungszeiten aufgrund des Wegfallens der Coin Rewards und der zu tiefen Transaktionsgebühren prognostiziert wird. Auf die Difficulty und den Schwellenwert wird nicht eingegangen, obwohl diese Faktoren für den Erhalt des zehn Minuten Durchschnittes beim Hinzufügen neuer Blocks verantwortlich sind, was wiederum eine zentrale Eigenschaft des Bitcoin-Systems darstellt. Falls die durchschnittliche Bestätigungszeit in einer Periode von 2'016 neuen Blocks also höher liegt, wird die Difficulty durch die Erhöhung des Schwellenwertes reduziert. Die Schlussfolgerung von Auer (2019) ist in diesem Zusammenhang nicht sinnvoll, weil sie die Difficulty-Anpassung nicht berücksichtigt.

Die Eignung von Bitcoin als Zahlungsmittel ist eine weitere in der Literatur diskutierte Thematik. Diese wird von Chiu und Koeppl (2017) zwar analysiert, jüngste Entwicklungen wie Second-Layer Lösungen werden aber im Hinblick auf die Probleme bezüglich der Skalierbarkeit und der Geschwindigkeit der Transaktionsbestätigung nicht berücksichtigt, obwohl solche Alternativen bereits vor 2017 vorgeschlagen wurden[6]. Dies erschwert es, aus der Studie die Zukunft der Zahlungsmittelfunktion von Bitcoin abzuschätzen. Das Lightning Netzwerk wurde bereits von Poon

[6]Ursprünglich von Poon und Dryja (2016).

und Dryja (2016) hervorgebracht und bietet Lösungen für sicherere und effizientere Transaktionen an. Deshalb wurde die Studie von Chiu und Koeppl (2017) durch solche ergänzt, die auf diese Lösungsansätze eingehen (Poon und Dryja (2016); Auer (2019); Lys et al. (2019); Miraz und Donald (2019*a*); Miraz und Donald (2019*b*); Berentsen und Schär (2017)). Diese ermöglichen die Ableitung möglicher Zukunftsentwicklungen bezüglich Skalierbarkeit und Bestätigungszeiten bei Transaktionen. Es bestehen also Lösungsansätze, die sich auf die von Chiu und Koeppl (2017) in Frage gestellte Zahlungsmittelfunktion von Bitcoin positiv auswirken könnten. Ein Netzwerk von Zahlungskanälen ermöglicht es, viel mehr Transaktionen abzuwickeln, und dies beinahe ohne Wartezeit für Transaktionsbestätigungen. Die Skalierbarkeit von Bitcoin kann mit solchen Off-Blockchain Transaktionen erhöht und das Gegenparteirisiko eliminiert werden (Poon und Dryja (2016)).

In der Literatur ist Double-Spending ein oft diskutiertes Thema. Von Chiu und Koeppl (2017) wird Confimation Lag als eine Möglichkeit vorgeschlagen, Double-Spending Anreize zu reduzieren. Laut Kang (2019) ist dies aber auch ohne Confirmation Lag möglich. Wenn der Verlust einer Wallet ohne Double-Spending Vorfälle (guter Ruf aufgrund der Historie) den kurzfristigen Nutzen aus Double-Spending übersteigt, wird der Angreifer kein Double-Spending mit einer guten Wallet betreiben. Der Verlust resultiert daraus, dass ein Angreifer nach dem Entdecken eines Angriffs fortan lediglich mit einer schlechten Wallet handeln kann. Kang (2019) untersucht verschiedene Gleichgewichte, die Double-Spending Anreize bestimmen. Auch Auer (2019) stellt Bedingungen auf, unter welchen ein Angriff nicht lohnenswert ist. Die Analyse dieser Studien hat gezeigt, dass Anreizsysteme hinsichtlich Double-Spending und der Sicherheit von Transaktionen bedeutend sind.

Die Erkenntnisse basieren jedoch auf Annahmen, die nicht immer realistisch sind. Auer (2019) geht davon aus, dass die Wahrscheinlichkeit für eine Hard Fork null beträgt ($\Pi^{HF} = 0$), obwohl die Regel der längsten Kette in der Vergangenheit in einigen Fällen missachtet wurde. Die Annahme einer positiven Wahrscheinlichkeit, oder die Analyse beider Fälle

wäre in diesem Fall aufschlussreicher. Bei einer positiven Wahrscheinlichkeit für eine Hard Fork wäre Double-Spending schwieriger, wodurch die Kosten der Verhinderung eines Angriffs gemäss dem Modell von Auer (2019) entsprechend sinken würden. Diese Zusammenhänge zeigen, dass je nach getroffenen Annahmen unterschiedliche Erkenntnisse resultieren können.

Auch bei 51%-Angriffen sollte genauer untersucht werden, ob der Besitz der Mehrheit der Gesamtrechenleistung einen Angriff begünstigt. Obwohl die generelle Annahme dafürspricht (Bitcoin Wiki (2019); Budish (2018)), gibt es abschreckende Aspekte, wie die Reduktion des Wertes des Bitcoinbestandes eines Angreifers (Budish (2018)). Ausserdem ist es entscheidend, welche ökonomische Bedeutung Bitcoin erlangen kann. Budish (2018) besagt, dass für einen Majority Attack eine grosse ökonomische Bedeutung von Bitcoin – beispielsweise in Form einer Wertspeicherfunktion – entscheidend ist. Diese wird aber nicht nur von Budish (2018), sondern auch von Berentsen und Schär (2017) in Frage gestellt. Aufgrund dieser Argumente scheint ein Majority Attack, der allein auf einen ausreichenden Besitz an Gesamtrechenleistung zurückgeführt werden kann, unrealistisch oder zumindest nicht derart dramatisch zu sein. Denn Berentsen und Schär (2017) betonen, dass das Abwarten von Bestätigungen dieses Problem bereits reduzieren kann.

In einigen Studien wird aufgrund bestehender Problemzonen vorgeschlagen, den zukünftigen Fokus nicht auf eine komplette Dezentralisierung zu richten. Laut Auer (2019) soll die Optimierung bestehender Systeme mit Hilfe der Technologie angestrebt werden, wobei Choi et al. (2018) ein System ohne zentrale Koordinationsmechanismen als unrealistisch erachten. Aufgrund der technologischen Fortschritte – auf welche unter anderem auch Auer (2019) in Form von Second-Layer Lösungen hindeutet – sollte keine derart ausschliessende Aussage über die Zukunft von Krytowährungen und der Blockchain-Technologie gemacht werden. Dies würde dem Urgedanken von Bitcoin, Transaktionen ohne zentrale Instanz abzuhandeln, widersprechen (Nakamoto (2008)). Ausserdem sind Second-Layer Lösungen – wie zum Beispiel durch das Lightning Netzwerk ermöglichte

Atomic Swaps – relativ jung und noch in der Entwicklungsphase (Miraz und Donald (2019*a*)).

Atomic Swaps sind zudem ein Gegenargument auf die Aussage von Böhme et al. (2015), das Gegenparteirisiko sei eine der Schwächen des Bitcoin-Systems. Atomic Swaps können Schwächen bezüglich der Skalierbarkeit von Kryptowährungen reduzieren und den Verlust von Coins an die Gegenpartei verhindern (Lys et al. (2019)). Ausserdem finden die Transaktionen abseits der Blockchain statt, wodurch deren Kapazität weniger belastet wird (Berentsen und Schär (2017)). Nebst anderen Risiken wie das Marktrisiko oder das Shallow Markets Problem sehen Böhme et al. (2015) auch Schwächen bezüglich des Datenschutzes und der Privatsphäre. Dies deshalb, weil in den Transaktionen der Public Key preisgegeben wird und allenfalls die Transaktionshistorie rekonstruiert und einem bestimmten Nutzer zugeordnet werden könnte. Jedoch werden im Bitcoin-System keine Informationen preisgegeben, die eine Transaktion einem bestimmten Individuum direkt zuordnen lassen würden (Conti et al. (2018)). Beim Public Key handelt es sich lediglich um ein Pseudonym. Hinzu kommt der Private Key, der ausschliesslich im Besitz der Person bleibt, die das Pseudonym erstellt hat und als Identitätsnachweis dient (Berentsen und Schär (2017)). Conti et al. (2018) empfehlen, für jede Transaktion ein neues Schlüsselpaar zu verwenden, um die Zuordnung einer Reihe von Transaktionen einem spezifischen Pseudonym zu verhindern, um so die Sicherheit zu erhöhen.

Ein oberflächlicher Vergleich ist zudem der Vergleich der Geschwindigkeit von Transaktionsbestätigungen. Weil bei Litecoin im Schnitt alle 2.5 Minuten ein neuer Block erzeugt wird, wird behauptet, dass Litecoin im Vergleich zu Bitcoin vier Mal schneller ist (Böhme et al. (2015)). Doch wird nicht beachtet, dass für die gleiche Sicherheit bei Litecoin schlicht mehr Bestätigungen benötigt werden. Anhand eines Beispiels aus Cryptowelt (2019) und der Plattform Bitstamp wurde gezeigt, dass bei Bitcoin drei, bei Litecoin hingegen sechs Bestätigungen abgewartet werden. In der Praxis sind bei Litecoin für die Verifizierung einer Transaktion also mehr Bestätigungen notwendig.

Am Beispiel der Kimchi-Prämie zeigen Choi et al. (2018), dass Preisdifferenzen nur zu einem bestimmten Grad durch die Mikrostruktur einer Kryptowährung erklärt werden können. In Europa waren Mikrostruktureffekte wie Bitcoin-Volatilität, Transaktionsgebühren und Bestätigungszeiten tiefer als in Südkorea. In der Studie wird festgestellt, dass der Faktor der ökonomischen Freiheit diesen Unterschied erklären kann und negativ mit der Bitcoin-Prämie korreliert. Dabei werden verschiedene Faktoren in Anlehnung an das Fraser Institute (2019) für die Bestimmung der ökonomischen Freiheit verwendet, wie beispielsweise Kapitalverkehrskontrollen. Bei Ländern mit relativ tiefer ökonomischer Freiheit wurden höhere Prämien festgestellt (Choi et al. (2018)). In Südkorea war dies bis Anfang 2018 der Fall. Zu erwähnen ist allerdings, dass die Kimchi-Prämie kontinuierlich zu sinken begann, nachdem die Skepsis der südkoreanischen Regierung gegenüber Kryptowährungen ab 2018 abgenommen hatte und immer mehr Regulierungen implementiert wurden (Oh (2018)).

Heute sind die Preise sehr ähnlich, was in der Detailanalyse der Studie von Choi et al. (2018) am Beispiel von jeweils einer Exchange aus den USA und Südkorea gezeigt wurde. Die Kimchi-Prämie ging ab 2018 zurück, obwohl die Kontrolle durch Regulierungen gestiegen ist. Dies spricht laut Oh (2018) gegen den gegensätzlichen Zusammenhang zwischen der ökonomischen Freiheit und den Prämien. Verantwortlich für die Kimchi-Prämie seien an erster Stelle drei Faktoren: Unterschiede in den Returns der Kryptowährung, die Zinssätze der Landeswährungen und die erwarteten Wechselkurse der Kryptowährung in Südkorea und den USA. Die Kimchi-Prämie sei also nicht ausschliesslich durch die ökonomische Freiheit zu erklären.

Die untersuchte ökonomische Literatur behandelt verschiedene Bitcoin und Blockchain spezifische Aspekte, wie das Vertrauen in die Blockchain-Technologie, die Zahlungsmittelfunktion von Bitcoin, Probleme wie Double Spending und Risikofaktoren, Transaktionsgebühren oder Preisdifferenzen zwischen verschiedenen Märkten für Kryptowährungen. Dabei werden oft die Grenzen, an welche Kryptowährungen stossen, analysiert

und alternative Designs für Kryptowährungen vorgeschlagen, um Probleme wie beispielsweise Double-Spending oder lange Bestätigungszeiten zu verhindern (Chiu und Koeppl (2017); Böhme et al. (2015)). Die angesprochenen Problemzonen sind wichtige Aspekte, da diese oft in Zusammenhang mit der Mikrostruktur von Kryptowährungen stehen. Jedoch wurden viele kontroverse Aussagen, Annahmen und Schlussfolgerungen festgestellt.

Ausserdem scheint, dass einige Probleme von Kryptowährungen dank den fortschreitenden technologischen Entwicklungen lösbar sind. Aus diesem Grund wurde in der Kritik der jeweiligen Studien auf Second-Layer Lösungen eingegangen, um die Lösbarkeit von Problemen, wie die begrenzte Skalierbarkeit und die langen Bestätigungszeiten bei Bitcoin-Transaktionen, hervorzuheben (Auer (2019); Lys et al. (2019); Miraz und Donald (2019*a*); Miraz und Donald (2019*b*); Berentsen und Schär (2017)). In der vorliegenden Arbeit wurde dabei vornehmlich auf das Lightning-Netzwerk eingegangen und ein Anwendungsbeispiel in Form von Atomic Swaps angesprochen. Aufgrund der Analyse kann abgeleitet werden, dass Second-Layer Lösungen und vor allem Off-Blockchain Transaktionen das Potenzial haben, Transaktionen sicherer, schneller und effizienter zu gestalten. Eine erhöhte Skalierbarkeit und kürzere Transaktionszeiten wären für die in Frage gestellte Tauschmittelfunktion von Bitcoin (Chiu und Koeppl (2017); Berentsen und Schär (2017)) vorteilhaft. Die Entwicklung solcher Lösungsansätze ist für die Zukunft von Bedeutung. Wie Miraz und Donald (2019*a*) erwähnen, sind Second-Layer Lösungen relativ jung und noch in der Entwicklungsphase. Aufgrund der Aktualität der Thematik und der ausgewählten Studien war es schwierig, noch mehr vergleichbare Papiere zu finden, die eine direkte Stellung zu den ausgewählten Studien nehmen. In künftigen Studien sollte die Thematik also weiter analysiert und die neuesten Entwicklungen aufgezeigt werden.

6 Konklusion

In der vorliegenden Arbeit wurde die ökonomische Literatur zum Thema Blockchain und Kryptowährungen untersucht. Bitcoin als populärste und in der bestehenden Literatur am häufigsten diskutierte Kryptowährung stand dabei im Fokus der Analyse. In einem ersten Schritt wurde die bestehende ökonomische Literatur zusammengestellt. Dabei stand nebst der Zusammenstellung ökonomischer Aspekte auch die kritische Beurteilung einiger Zusammenhänge und Schlussfolgerungen in den untersuchten Studien im Vordergrund. In der Literaturübersicht wurden Themen wie die Eignung von Kryptowährungen als Zahlungsmittel und damit verbundene Probleme wie Double-Spending, die Transaktionssicherheit, die Belohnungskomponenten der Miner, Risikofaktoren und Preisunterschiede bei Kryptowährungen unter die Lupe genommen. Bereits die Literaturübersicht ergab dabei Diskussionsstoff. Kontroverse Aussagen wurden anhand der bestehenden Literatur kritisiert. Ein Beispiel stammt von Chiu und Koeppl (2017), die eine ausschliessliche Belohnung der Miner durch neu geschöpfte Bitcoins vorschlagen. Doch Transaktionsgebühren sind notwendig, um die Mining-Anreize aufrecht zu erhalten (Berentsen und Schär (2017)), aber auch um DDoS Angriffe zu verhindern (Saad et al. (2018)). Aufgrund der begrenzten Bitcoin-Schöpfung werden Coin Rewards einmal gänzlich wegfallen und die Bedeutung der Transaktionsgebühren als Belohnungskomponente weiter steigen.

Bezüglich der unmittelbaren Tauschmittelfunktion von Bitcoin wurde festgestellt, dass Problemen wie der begrenzten Skalierbarkeit und der vergleichsweise langen Bestätigungszeiten durch Second-Layer Lösungen entgegengewirkt werden kann (Auer (2019); Lys et al. (2019); Miraz und Donald (2019*a*); Miraz und Donald (2019*b*); Berentsen und Schär (2017)). Anwendung finden Second-Layer Lösungen beispielsweise in Form von Atomic Swaps, die durch das Lightning Netzwerk ermöglicht werden und Mängel bezüglich der Interoperabilität zwischen verschiedenen Blockchains und der Skalierbarkeit von Kryptowährungen verbessern sollen. Dezentrale Zahlungsnetzwerke ermöglichen zudem Off-Blockchain Transaktionen, die die Belastung der maximalen Blockgrösse reduzieren. Off-

Blockchain Transaktionen gehen nicht alle einzeln, sondern aggregiert in die Blockchain ein (Berentsen und Schär (2017)). Second-Layer Lösungen wie das Lightning Netzwerk werden jedoch nicht in jeder Studie berücksichtigt (vgl. Chiu und Koeppl (2017)), obwohl diese Lösungen für erwähnte Probleme wie die begrenzte Skalierbarkeit vorschlagen (vgl. Poon und Dryja (2016)). Die Erkenntnis daraus ist, dass dank den fortschreitenden Entwicklungen eine effizientere Anwendung der Blockchain-Technologie und der Kryptowährungen möglich ist. Des Weiteren wird die Wertspeicherfunktion von Bitcoin in Zusammenhang zu 51% Angriffen diskutiert. Ein 51% Angriff ist dann möglich, wenn Bitcoin eine grosse ökonomische Bedeutung - wie in Form einer Wertspeicherfunktion - erlangen kann (Budish (2018)). Doch gibt es Faktoren wie die grossen Wertschwankungen, die für die Wertspeicherfunktion von Bitcoin keine gute Voraussetzung darstellen (Berentsen und Schär (2017)). Die relativ tiefe Marktkapitalisierung von Bitcoin stellt diesbezüglich ein weiteres Gegenargument dar.

Bezüglich bestimmter Risikofaktoren wurde festgestellt, dass sie nicht derart dramatisch sind und bereits Lösungen existieren. Dem von Böhme et al. (2015) beschriebenen Gegenparteirisiko kann beispielsweise durch Atomic Swaps entgegengewirkt werden. Dabei muss das Protokoll versichern, dass keine Partei ihre Coins verliert (Lys et al. (2019)). Datenschutzspezifische Risiken aus der Studie von Böhme et al. (2015) werden kritisiert, weil die Verwendung eines neuen Schlüsselpaares für jede neue Transaktion die Zuordnung einer Reihe von Transaktionen einem spezifischen Pseudonym bereits verhindern kann (Conti et al. (2018)). Zudem ist der Private Key ausschliesslich im Besitz derjenigen Person, die das Pseudonym erstellt hat. Somit lassen sich Faktoren, die als Risiko dargestellt werden, widerlegen.

Die kritische Würdigung der bestehenden ökonomischen Literatur hat insgesamt gezeigt, dass zwar wichtige Aspekte analysiert, dabei aber einige entscheidende Faktoren unbeachtet gelassen werden. Bei der Prognose von steigenden Bestätigungszeiten aufgrund der zu tiefen Transaktionsgebühren sowie der periodisch halbierten Coin Rewards im Bitcoin-System

(Auer (2019)) werden die Difficulty-Anpassung und der Schwellenwert missachtet. Das Problem der begrenzten Skalierbarkeit wird in der Literatur oft adressiert. Während Chiu und Koeppl (2017) diesbezüglich nicht auf Second-Layer Lösungen verweisen, gehen einige Studien darauf ein und stellen fest, dass solche Lösungsansätze für die Effizienz und Sicherheit von Transaktionen wichtig sind (vgl. Poon und Dryja (2016); Auer (2019); Lys et al. (2019); Miraz und Donald (2019*a*); Miraz und Donald (2019*b*); Berentsen und Schär (2017)). Ein weiteres Beispiel für eine kritische Annahme stammt aus der Studie von Auer (2019), in der die Wahrscheinlichkeit für eine Hard Fork von null angenommen wird, obwohl die Regel der längsten Kette in einigen Fällen in der Vergangenheit missachtet wurde. Die Annahme einer positiven Wahrscheinlichkeit würde die Kosten der Verhinderung eines Double-Spending Angriffs gemäss Modell reduzieren.

Die bestehende ökonomische Literatur zur Blockchain und Kryptowährungen wurde anhand dieser und ähnlicher Kontroversen kritisch beurteilt. Die Erkenntnis der vorliegenden Arbeit ist, dass eine fundierte Analyse der ökonomischen Gegebenheiten notwendig ist, um mögliche Grenzen und Probleme der Blockchain-Technologie und Kryptowährungen feststellen zu können. Künftige Studien sollten die Existenz von Second-Layer Lösungen in Betracht ziehen, um die Zukunft aktueller Probleme - wie die angesprochene begrenzte Skalierbarkeit von Bitcoin - prognostieren zu können.

Literaturverzeichnis

Auer, R. (2019), 'Beyond the Doomsday Economics of 'Proof-of-Work' in Cryptocurrencies', *BIS Working Paper Series* (765).

Badev, A. I. and Chen, M. (2014), 'Bitcoin: Technical Background and Data Analysis'.

Berentsen, A. and Schär, F. (2017), 'Bitcoin, Blockchain und Kryptoassets', *BoD - Books on Demand, Norderstedt* .

Bitcoin Wiki (2019), 'Majority Attack'. `https://en.bitcoin.it/wiki/Irreversible_Transactions#Majority_attack`. Abgerufen am: 26.10.2019.

Bithumb (2019), 'Bitcoin/KRW Kurs'. `https://en.bithumb.com`. Abgerufen am: 18.12.2019.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), 'Bitcoin: Economics, Technology, and Governance', *Journal of Economic Perspectives* **29**(2), 213–38.

Budish, E. (2018), 'The Economic Limits of Bitcoin and the Blockchain', Technical report, National Bureau of Economic Research.

Chiu, J. and Koeppl, T. V. (2017), 'The Economics of Cryptocurrencies - Bitcoin and Beyond', *Available at SSRN 3048124* .

Choi, K. J., Lehar, A. and Stauffer, R. (2018), 'Bitcoin Microstructure and the Kimchi premium', *Available at SSRN 3189051* .

Coinbase (2019), 'Bitcoin/US-Dollar Kurs'. `https://www.coinbase.com`. Abgerufen am: 18.12.2019.

CoinMarketCap (2019), 'Marktkapitalisierung Bitcoin in US-Dollar'. `https://coinmarketcap.com/de/currencies/bitcoin/`. Abgerufen am: 24.12.2019.

Conti, M., Kumar, E. S., Lal, C. and Ruj, S. (2018), 'A Survey on Security and Privacy Issues of Bitcoin', *IEEE Communications Surveys & Tutorials* **20**(4), 3416–3452.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016), 'BlockChain Technology: Beyond Bitcoin', *Applied Innovation* **2**(6-10), 71.

Cryptowelt (2019), 'Börsen - Anzahl Bestätigungen'. `https://cryptowelt.ch/Glossar/boersen-anzahl-bestaetigungen/#Bitstamp`. Abgerufen am: 14.12.2019.

Fraser Institute (2019), 'Economic Freedom: Approach'. `https://www.fraserinstitute.org/economic-freedom/approach`. Abgerufen am: 05.12.2019.

Huberman, G., Leshno, J. D. and Moallemi, C. (2017), 'Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System', *Columbia Business School Research Papers* (17-92).

Johnson, B., Laszka, A., Grossklags, J., Vasek, M. and Moore, T. (2014), 'Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools', *in* 'International Conference on Financial Cryptography and Data Security', Springer, pp. 72–86.

Kang, K. and Lee, S. (2019), 'Money, Cryptocurrency, and Monetary Policy', *Available at SSRN 3303595* .

Kang, K.-Y. (2019), 'Cryptocurrency and Double Spending History: Transactions with Zero Confirmation', *Available at SSRN 3369306* .

Li, W., Andreina, S., Bohli, J.-M. and Karame, G. (2017), 'Securing Proof-of-Stake Blockchain Protocols', *in* 'Data Privacy Management, Cryptocurrencies and Blockchain Technology', Springer, pp. 297–315.

Loader, B. D. and Dutton, W. H. (2012), 'A Decade in Internet Time', *Information, Communication & Society* **15**(5), 609–615.

Lys, L., Micoulet, A. and Potop-Butucaru, M. (2019), 'Atomic Swapping Bitcoins and Ethers', *SRDS 2019 - 38th International Symposium on Reliable Distributed Systems* .

Mattila, J. (2016), 'The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures', *ETLA Working Papers* (38).

Miraz, M. and Donald, D. C. (2019*a*), 'Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities', *Annals of Emerging Technologies in Computing (AETiC) Vol* **3**.

Miraz, M. and Donald, D. C. (2019*b*), 'LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications', *in* 'Proceedings of the 2019 3rd International Conference on Information System and Data Mining', ACM, pp. 185–189.

Moore, T. and Christin, N. (2013), 'Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk', *in* 'International Conference on Financial Cryptography and Data Security', Springer, pp. 25–33.

Möser, M. and Narayanan, A. (2019), 'Effective Cryptocurrency Regulation Through Blacklisting', *Princeton University* .

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'. `http://bitcoin.org/bitcoin.pdf`.

Oh, J. H. (2018), 'The Foreign Exchange Market With the Cryptocurrency and Kimchi Premium', *The 22nd Biennial Conference of the International Telecommunications Society: "Beyond the boundaries: Challenges for business, policy and society", June 24th - 27th, 2018, Seoul, Korea* .

Poon, J. and Dryja, T. (2016), 'The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments'. `https://lightning.network/lightning-network-paper.pdf`. Abgerufen am: 12.12.2019.

Saad, M., Njilla, L., Kamhoua, C., Kim, J., Nyang, D. and Mohaisen, A. (2019), 'Mempool Optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems', *in* '2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)', IEEE, pp. 285–292.

Saad, M., Thai, M. T. and Mohaisen, A. (2018), 'POSTER: Deterring DDoS Attacks on Blockchain-based Cryptocurrencies through Mempool Optimization', *in* 'Proceedings of the 2018 on Asia Conference on Computer and Communications Security', ACM, pp. 809–811.

Saleh, F. (2019), 'Blockchain Without Waste: Proof-of-Stake', *Available at SSRN 3183935* .

Schlatt, V., Schweizer, A., Urbach, N. and Fridgen, G. (2016), 'Blockchain: Grundlagen, Anwendungen und Potenziale'.

Sixt, E. (2017), 'Bitcoins und andere dezentrale Transaktionssysteme', *Blockchains als Basis einer Kryptoökonomie, Wiesbaden* .

Vora, G. (2015), 'Cryptocurrencies: Are Disruptive Financial Innovations Here?', *Modern Economy* **6**(07), 816.

Xie, A. (2019), '51% Attacks for Rent - The Consequence of a Liquid Mining Market'. `https://hackernoon.com/51-attacks-for-rent-the-consequence-of-a-liquid-mining-market-c37d9ca84008`. Abgerufen am: 16.12.2019.

Yim, S., Kim, G.-J. and Kim, M. (2018), 'The Korean Premium: Cryptocurrency - Arbitrage Phenomenon in Korea', *Includes Chapter News* **31**(1), 30.

Abbildungsverzeichnis