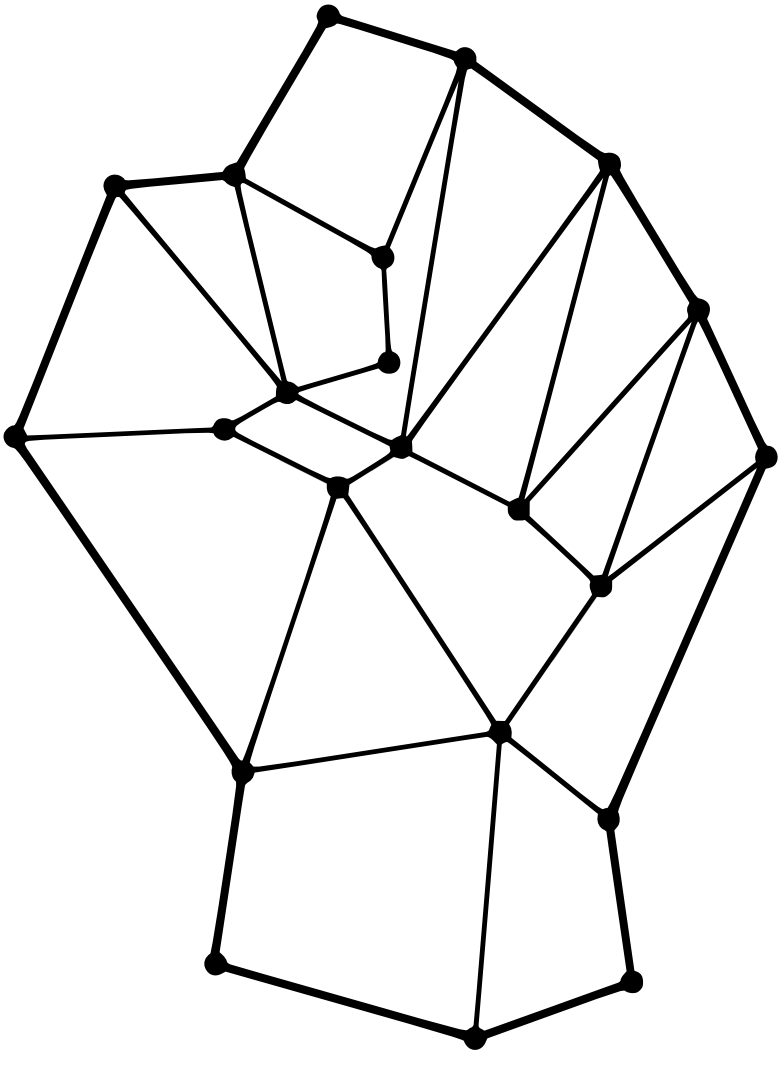
KRYPTOÖKONOMIE

GRUNDPRINZIPIEN VON BITCOIN



ERIC VOSKUIL

Herausgegeben und illustriert von James Chiang

KRYPTOÖKONOMIE

Grundprinzipien von Bitcoin

Eric Voskuil

Kryptoökonomie, Grundprinzipien von Bitcoin, 2. Ausgabe

Version 1.2.3, Portable Document Format (PDF)

Herausgeber
Veröffentlicht in den Vereinigten Staaten von Amerika durch Eric Voskuil.

Autor
Eric Voskuil

Herausgeber und Illustrator
James Chiang

Deutsche Übersetzung
Kevin Abramczyk

ISBN: 979-8-9869946-5-9

Autor

Eric Voskuil

Eric Voskuil leistete einen maßgeblichen Beitrag zu Libbitcoin[1], einem freien Open-Source, High-Performance Bitcoin-Developer-Toolkit. Er machte seinen Abschluss in Informatik am Rensselaer Polytechnischen Institut[2], verkaufte sein erstes Startup, DesktopStandard[3], an Microsoft[4] und sein zweites, BeyondTrust[5], an Veritas Capital[6]. Seit Anfang 2014 arbeitet er in der Bitcoin-Core-Entwicklung und spricht weltweit auf Konferenzen und Meetups. Darüber hinaus ist er mehrfacher Unternehmensgründer, Business Angel, Kampfsportler, begeisterter Motorradfahrer, Weltreisender und ehemaliger U.S. Navy[7]-Kampfjetpilot.

Anfang 2020 hielt er die CryptoEcon[8] in Hanoi, die erste Konferenz speziell für kryptoökonomische Theorie, war Mitgründer des Libbitcoin-Instituts[9] zur finanziellen Förderung von Bitcoin-Entwicklung und -Bildung, sponserte die erste Bitbikers[10]-Motorradtour durch Nordvietnam und veröffentlichte die erste Ausgabe von *Kryptoökonomie*.

Referenzen

[1] https://libbitcoin.info

[2] https://rpi.edu

[3] https://www.eweek.com/enterprise-apps/microsoft-buys-desktopstandard

[4] https://microsoft.com

[5] https://beyondtrust.com

[6] https://veritascapital.com

[7] https://www.navy.mil

[8] https://cryptoecon.org

[9] https://libbitcoininstitute.org

[10] https://bitbikers.org

Herausgeber & Illustrator

James Chiang

James ist ein Open-Source-Entwickler, der sowohl zu Libbitcoin[1] als auch zu Bitcoin Core[2] beigetragen hat. Er las sein erstes Kryptoökonomie-Kapitel, Dedicated Cost Principle[3], Anfang 2018 und begann zum besseren Verständnis Zeichnungen der zugrunde liegenden Prinzipien anzufertigen. Im Moment forscht er über die formale Sicherheit von Smart Contracts. James ist Doktorand der Informatik an der technischen Universität Dänemark[4] und ehemaliger Luft- und Raumfahrtingenieur am Jet Propulsion Lab[5].

Referenzen

[1] https://libbitcoin.info

[2] https://bitcoincore.org

[3] Kapitel: Dediziertes Kostenprinzip

[4] https://www.dtu.dk/english

[5] https://www.jpl.nasa.gov

Übersetzer
Kevin Abramczyk

Es war wohl im Nachhinein der Höhepunkt meines persönlichen Bitcoin-Maximalismus, als mir der Spotify-Algorithmus im Sommer 23 das von Max Hillebrand eingesprochene Hörbuch[1] von Cryptoeconomics einspielte. Freiwillig hätte ich das Buch natürlich nie gelesen, trägt es doch den Begriff „Crypto“ im Titel. Wider Erwarten war diese unromantische und rationale Sammlung einiger oft aber regelmäßig falsch wiedergegebener Aspekte rund um Bitcoin aber genau das, was ich zu diesem Zeitpunkt brauchte.

Dass Bitcoin nicht die gesamte Energie der Menschheit verbraucht oder dass Proof-of-Stake keine vergleichbare Alternative zu Proof-of-Work darstellt, muss man einem Fachkundigen heute nicht mehr erklären. Warum die Änderung der Blockgröße das Skalierungsproblem aber immer nur verschiebt und nie löst, dass das Halten von BTC reine Spekulation und keine Investition ist und dass der Staat Bitcoin sehr wohl verbieten kann, gilt aber eher als unpopuläre Meinung. Das Erfrischende an diesem Buch ist nun genau das, es hat mit Meinungen nicht viel zu tun.

Ausgehend von den grundlegenden kryptodynamischen Prinzipien, die Bitcoin zu dem machen, was es ist, beschreibt Eric Voskuil den Markt und die in ihm wirkenden Kräfte aus der Sicht der Schule der österreichischen Nationalökonomie. Dabei analysiert er sachlich und nüchtern den Zusammenhang von Produktion und Konsum, die Wechselwirkungen zwischen Geld und Kredit, den Unterschied zwischen Bitcoin und Shitcoin und kommt schließlich nicht umher, selbst in den Klassikern von Mises und

Referenzen

[1] https://open.spotify.com/show/2y6oTLWiId7JmUp6pTjPOS

Rothbard Unstimmigkeiten aufzudecken, wenn er z.B. erläutert, warum Warengelder nicht der Preisinflation unterliegen.

Dieses Buch ist kein Roman, weder in englischer noch in deutscher Sprache. Es ist ein Nachschlagewerk für diejenigen, denen ein ungefähres Verständnis wirtschaftlicher Zusammenhänge nicht ausreicht. Für diejenigen, die sich nicht auf schmissige Werbeslogans und Hopium verlassen, sondern genau wissen wollen, welche Kräfte die Wirtschaft und Bitcoin beeinflussen. Als Freund der deutschen Sprache habe ich versucht überall dort, wo es möglich und angebracht war, deutsche Begriffe zu verwenden. So schafften es heutzutage wenig gebräuchliche Begriffe wie Kartellierung (Pooling) oder Kooptierung (co-option) in den Text. Aus Replay Protection wurde der Wiederholungsschutz aber eine Übersetzung von Coin oder Proof-of-Work war mir dann doch zu viel des Guten. Die meisten externen Links wurden auf deutschsprachige Alternativen umgesetzt, einige wenige inzwischen tote Links wurden neu belegt. Ich danke dem Übersetzer der italienischen Ausgabe, parsevalbtc[1], der mich mit der Idee für diese Übersetzung angesteckt hat, ebenso wie juniormind[2] für das Lektorat, ohne welches ich einige der von mir übersetzten Sätze nur halb so gut verstanden hätte.

Ich hoffe, dass dieses Buch der deutschsprachigen Bitcoin- und Crypto-Community dabei hilft, zielgerichteter sowohl über die Möglichkeiten als auch die Probleme und die technischen Grenzen von Bitcoin sprechen zu können. Fragen, Anregungen und Ergänzungen[3] sind in diesem Austausch ebenfalls herzlich willkommen. Bitcoin ist ein langer Hebel zur Verteidigung des Privateigentums und des freien Marktes gegen den Staat, so viel ist sicher. Allerdings ist dieser Nutzen nicht kostenlos. Bitcoins Wert beruht weder auf dessen Knappheit, noch stammt er aus der Energie, die für das Mining aufgewendet wird. Wert ist subjektiv und das gilt auch für Bitcoin. Kryptoökonomie hilft

Referenzen

[1] https://x.com/parsevalbtc/

[2] https://x.com/Juniormind1

[3] https://x.com/ZitadelleUM

all die Eigenschaften zu verstehen, aufgrund derer ihm seine Nutzer einen seit vielen Jahren wachsenden Wert beimessen.

Danksagungen

Dieses Projekt begann in Form von Tweets[1] und Posts im Wiki des Libbitcoin[2] Software-Repositorys[3]. Irgendwann gab es genügend Inhalt und Interesse, sodass ich Anfragen für ein Buch bekam. Dann kamen Angebote, Übersetzungen anzufertigen. Schließlich unternahm **James Chiang** den Versuch einer Veröffentlichung. Er hatte die Zusammenstellung nahezu abgeschlossen, einschließlich seiner Illustrationen. Seine aufschlussreichen Fragen brachten mich dazu, das Inflationsprinzip[4] zu überdenken, was mich zu einer wichtigen ökonomischen Einsicht brachte. Dennoch machten meine ständigen Erweiterungen und Änderungen zu dieser Zeit eine Fertigstellung nahezu unmöglich. Schließlich machte sich James auf zu größeren Zielen, seine Arbeit und Illustrationen trugen aber maßgeblich zur Veröffentlichung bei. Ich kann ihm nicht genug danken.

Das vergangene Jahr über arbeitete **Fabrizio Armani** an der italienischen Übersetzung. Sein Feedback half mir die vorliegende Ausgabe zu verbessern. Sein Unbehagen mit dem Sparverhältnis[5] führte schließlich dazu, dass ich die Schlussfolgerung zurückzog. Ich hatte das Glück, dass er mich aktiv bei der Überarbeitung dieser Ausgabe unterstützt hat. Beim Versuch eine kryptoökonomische Schlussfolgerung darzulegen will ich stets mein größter Kritiker sein. Dennoch haben mir James und Fabrizio klar gezeigt, wie wertvoll es doch ist, mit anderen engagierten Beteiligten zusammenzuarbeiten.

Bitcoin begann für mich mit Libbitcoin. Unmittelbar nachdem ich angefangen hatte, flog ich nach Spanien, um mich mit **Amir Taaki** zu treffen. Er hatte die Libbitcoin-

Referenzen

[1] https://twitter.com

[2] https://libbitcoin.info

[3] https://github.com/libbitcoin/libbitcoin-system/wiki/Cryptoeconomics

[4] Kapitel: Inflationsprinzip

[5] Kapitel: Sparverhältnis

Community gegründet und leitete das Projekt bis zu seinem Abstecher nach Rojava[1]. Er war äußerst geduldig mit mir, während ich meine C++-Fähigkeiten auffrischte und die Eigenheiten von Bitcoin erlernte. Libbitcoin ist eine besondere Community innerhalb des Universums der Core-Entwicklung und Amir gebührt die Anerkennung dafür. Es war der Versuch den Hype um Bitcoin mit meinen persönlichen Erfahrungen in Einklang zu bringen, der zu Kryptoökonomie führte. Entscheidungen, die in der Entwicklung getroffen werden, stehen in direktem Zusammenhang mit den wirtschaftlichen Grundlagen. Wir mussten erklären, was wir uns selbst und anderen antaten. Letztendlich führten sein Input und seine Erkenntnisse zu dieser Arbeit, daher ist es nur passend und ich freue mich sehr darüber, dass er sich dazu bereiterklärt hat, das Vorwort[2] zu verfassen.

Ich verweise häufig auf **Phillip Mienk** als die klügste Person, die ich kenne. Er wechselte aus dem Doktorandenprogramm der renommierten University of Illinois, Urbana-Champaign Computer Science[3] in einen Microsoft[4]-Talentpool. Zu dieser Zeit baute ich gerade ein neues Entwicklungsteam auf und war nicht scharf darauf, den College-Angestellten zu schulen, den Microsoft mir vor die Nase gesetzt hatte. Ich erkannte allerdings schnell, welches Glück ich tatsächlich hatte. Als ich ging, folgte er mir zu einem dritten Startup und and dem Tag, als es dicht machte, folgte er mir zu Libbitcoin. Seit einem Jahrzehnt ist er ein wichtiger Partner, immer in der Lage den komplexesten Problemen direkt auf den Grund zu gehen. Ich bin dankbar für seine Unterstützung während einiger schwerer Zeiten und letztlich für seinen wertvollen Beitrag zu dieser Arbeit.

Neill Miller fand irgendwie zu Libbitcoin, machte wichtige Beiträge zu unserem Wallet und unserer Server-API und betreute mehrere Jahre lang unsere Community-Server.

Referenzen

[1] https://en.wikipedia.org/wiki/Amir_Taaki

[2] Kapitel: Vorwort

[3] https://cs.illinois.edu

[4] https://microsoft.com

Kulpreet Singh spürte mich auf dem Baltic-Honeybadger[1] 2019 auf und fragte mich über Libbitcoin aus. Seitdem hat er wichtige Beiträge zu unserer Datenbank-Test-Suite geleistet und arbeitet weiterhin an Designverbesserungen in den darunterliegenden Speichermechanismen. Zusammen mit Phillip waren Neill und Kulpreet das Rückgrat von Libbitcoin. Ohne ihre Unterstützung wäre es mir nicht möglich, so viel Zeit mit dem Schreiben von Büchern zu verbringen, während ich eigentlich Code schreiben sollte.

Das Libbitcoin Institut[2] ist das geistige Produkt **Thomas Pacchias**. Tom brachte mich mit **Lucas Betschart** zusammen, um die Organisation zu dem Zweck aufzubauen, Geld für die Entwicklung von Libbitcoins freier Software[3] und die Bitcoin-Bildung zu sammeln. Er erledigte die ganze mühsame Arbeit, die erforderlich war, um den 501c3 Status[4] gegenüber der IRS zu erhalten. Bis heute ist die IRS ihrer Pflicht noch nicht nachgekommen, dennoch bleibt das Institut ein Werkzeug für die Unterstützung, die notwendig ist, um Bitcoins Wertversprechen[5] einzuhalten. Tom und Lucas waren großartige Unterstützer und gute Freunde.

Die erste Ausgabe von *Kryptoökonomie* wurde lediglich an die Teilnehmer der CryptoEcon[6] 2020 in Hanoi ausgegeben. Es sollte kurz danach online zum Verkauf angeboten werden aber das Leben kam dazwischen. Die Beilagen blieben in einem Motorrad-Laden auf der Tay Ho Street. Aber CryptoEcon, ein Projekt des Libbitcoin-Instituts, half die Botschaft zu verbreiten. Die Spenden von HODL Capital[7] (durch **Thomas Pacchia**) und Lemniscap[8] (durch **Roderik van der Graaf**) haben die Konferenz

Referenzen

[1] https://twitter.com/hashtag/bh2019?src=hashtag_click

[2] https://libbitcoininstitute.org

[3] https://de.wikipedia.org/wiki/Free_Software_Foundation

[4] https://www.irs.gov/charities-non-profits/charitable-organizations/exemption-requirements-501c3-organizations

[5] Kapitel: Wertversprechen

[6] https://cryptoecon.org

[7] https://www.21shares.com/en-eu/blog/hodl-capital-case-study

[8] https://lemniscap.com

erst möglich gemacht. Tom suchte mich auf der Building on Bitcoin[1] 2018 in Lissabon auf, Roderik erwischte mich beim Baltic Honeybadger 2019 in Riga. Sie ergriffen die Initiative und motivierten mich, das Buch zur Konferenz fertigzustellen.

Alle Personen aufzuzählen, die durch inspirierende Themen sowie konstruktive Kritik ihren Beitrag geleistet haben, ist nicht möglich. Unter ihnen sind Konferenz- und Meetup-Veranstalter, Podcaster, Teilnehmer und Zuhörer sowie ein scheinbar nicht enden wollender Strom an Twitter-Kommentatoren. Ich habe durch die Verfolgung fehlerhafter Ideen viel mehr gelernt als durch die fundierten. Doch ohne die gelegentlichen aufmunternden Worte ist so etwas viel schwieriger zu erreichen.

Abschließend möchte ich mich bei meinen Freunden und meiner Familie bedanken, die mich in dieser schwierigen Zeit unterstützt haben.

Referenzen

[1] https://building-on-bitcoin.com

INHALT

Inhalt

VORWORT

Vorwort
Von Amir Taaki

Krypto-Anarchie[1] ist weder eine Strategie zur Durchsetzung politischer Hegemonie noch zur Diskreditierung anderer möglicher Einstellungen oder Absichten. Sie ist lediglich eine Sammlung von Konzepten und Ideen, die taktisch dazu genutzt werden können, alternative Lebensweisen zu verwirklichen. Die Geschichte ist das Ergebnis menschlichen Wollens und Handelns. Dies geschieht allerdings immer innerhalb eines Rahmens aus Überzeugungen, Glaubensgrundsätzen und Darstellungen, der unserem Handeln eine Richtung und eine Bedeutung gibt. Auf diesem Wege versucht die Krypto-Anarchie, das Individuum mit leistungsstarken konzeptionellen Werkzeugen auszustatten, damit es seine eigenen kreativen Visionen erbauen kann.

Ökonomie ist wichtig, ist sie doch die Lehre der grundlegenden Mechanismen der menschlichen Handlung und von deren Konsequenzen. Vernünftige Ökonomen analysieren menschliche Aktivitäten und akzeptieren dabei, dass das Wissen begrenzt ist. Aus einer Reihe einfacher Annahmen, wie zum Beispiel, dass der Mensch handelt[2] und eine frühe Belohnung einer späteren vorzieht[3], werden mit Hilfe von Schlussregeln[4] Theoreme abgeleitet. Die Entwicklung dieser Theoreme ermöglicht es uns, komplexe Phänomene mit Hilfe einfacher Konstrukte zu analysieren und aufzugliedern.

Die Kryptowährung[5] entstand durch die Krypto-Anarchie sowie eine freie Marktwirtschaft, ist aber inzwischen über sich selbst hinausgewachsen und wurde zu

Referenzen

[1] https://de.wikipedia.org/wiki/Krypto-Anarchie

[2] https://en.wikipedia.org/wiki/Action_axiom

[3] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

[4] https://de.wikipedia.org/wiki/Schlussregel

[5] https://de.wikipedia.org/wiki/Kryptowährung

einem Phänomen unserer Zeit mit eigenartigen Wesenszügen. Dies hat uns gezwungen, unsere eigenen Vorstellungen und Annahmen darüber zu überdenken, wie diese Disziplinen miteinander zusammenhängen. Diese neue Lehre wird Kryptoökonomie genannt.

Kryptowährungen wie Bitcoin verkörpern zum ersten Mal in der Menschheitsgeschichte Geld, welches gleichzeitig global, nicht zensierbar und für jeden frei zugängig ist. Auch in der Anonymisierungstechnologie werden große Fortschritte erzielt, nicht nur für Kryptowährungen sondern auch für Finanzinstrumente und menschliche Aktivitäten im Allgemeinen. Kryptowährung ist daher ein einzigartiges Phänomen mit eigenen Merkmalen, die es wert sind, untersucht zu werden.

Die Bedeutung der Ökonomie liegt darin, uns ein Fenster zum Verständnis der Handlungen menschlicher Wesen zu geben. Das bedeutet, dass wir planen können, wo wir unsere Ressourcen und unser technisches Wissen einsetzen wollen. Der aktuellen Generation von Krypto-Unternehmen fehlt diese strategische Dimension und sie werden daher nicht in der Lage sein, die Vorteile aus neuen geopolitischen Trends zu nutzen. Derzeit gibt es zu viel Streuung hinsichtlich der Ziele – die Krypto-Industrie ist nicht selektiv genug.

Konzepte aus der Evolutionstheorie können uns helfen vorherzusagen, welche Organisationsstrategien sich langfristig durchsetzen werden. Die Fortpflanzungsstrategie[1] zum Beispiel erklärt, dass nach großen Massenaussterben diejenigen Organismen zuerst die Nischen besetzen, deren Arten eine hohe Zahl an Jungtieren haben, welche schnell heranwachsen und die nur wenig Ressourcen von den Eltern investieren müssen (r-Strategie)[2]. Sie werden jedoch langfristig von den Organismen verdrängt, die weniger Nachwuchs haben, besser an ihre Lebensumgebung

Referenzen

[1] https://de.wikipedia.org/wiki/Fortpflanzungsstrategie

[2] https://de.wikipedia.org/wiki/Fortpflanzungsstrategie#r-Strategie

angepasst sind und länger für das Heranwachsen benötigen (K-Strategie)[1]. Krypto-Organismen, die der K-Strategie folgen, sind diejenigen, die besser an die sich öffnenden ökonomischen Nischen angepasst sind.

Eine weitere Hypothese der Evolutionstheorie ist die Red-Queen-Hypothese[2] welche besagt, dass sich Organismen in einem fortwährenden Kampf um ihre Fortentwicklung befinden. Das heißt, dass wir uns ununterbrochen, in einem sich fortlaufend ändernden Umfeld, an sich ständig weiterentwickelnde Akteure anpassen und uns weiterentwickeln müssen.

Das tun wir, indem wir unser Wissen dazu anwenden, um Muster zu finden und konzeptuelle Modelle aufzubauen, wobei wir diese Modelle durch Feedback verändern, um ihre Genauigkeit zu erhöhen sowie die zugrundeliegenden Paradigmen zu erweitern.

Die gegenwärtige Auslese an Krypto-Unternehmen wird schon bald aussterben. An ihre Stelle wird eine neue Generation von Organisationen treten. Diese werden hochgradig anpassbar sein, abgestimmt auf geopolitische Trends und optimiert für das Überleben in einen Zustand des ständigen Ungleichgewichts. Um derartigen Bedingungen zu widerstehen, sollte diese Generation auf einer Synthese aus der Scharfsinnigkeit der Kryptoökonomie und der Krypto-Anarchie selbst gegründet werden – was im Kern ein recht einfacher Grundsatz ist: Der Motor des geschichtlichen Wandels ist nicht nur technologischer Fortschritt, sondern es sind auch Konzepte, Modelle und Ideen, die uns Macht über die materielle Realität verleihen.

Meine Erfahrungen mit Eric reichen zurück bis 2013, als wir mit der Arbeit an Bitcoin-Frameworks[3] begannen, welche sowohl schnell als auch gut skalierbar waren. Eric ist ein Entwickler, der mit Links die Arbeit eines ganzen Teams erledigen kann, um produktive

Referenzen

[1] https://de.wikipedia.org/wiki/Fortpflanzungsstrategie#K-Strategie

[2] https://de.wikipedia.org/wiki/Red-Queen-Hypothese

[3] https://github.com/libbitcoin

Software herzustellen – eine sehr seltene Fähigkeit. Außerdem verfügt er über eine weitreichende Lebenserfahrung, als Düsenjägerpilot der U.S. Navy ebenso wie als erfolgreicher Gründer mehrerer Unternehmen. Er vereint intensives praktisches Wissen mit einem fundierten theoretischen Unterbau sowie einem inbrünstigen Interesse nach Wissen, sowohl in der Politik als auch in der Ökonomie.

Erics einzigartige Einsichten in grundlegende Konzepte bieten uns ein unverzichtbares Rahmenwerk für die künftige Ausrichtung des Bereiches der Kryptoökonomie. Er wendet die rationale Wirtschaftstheorie konsequent auf Kryptowährungen an und wagt sich über finanzielle Aspekte hinaus, um zu erklären, wie das menschliche Handeln diese Zukunft prägt.

VORREDE

Vorrede

Das Vorliegende begann als ein Versuch zu vermeiden, dieselben Ideen immer wieder zu wiederholen – und das jeweils mit 140 Zeichen[1]. Diesem Umfeld entsprechend waren die Themen so kurz wie möglich und informell gehalten. Ich hatte nie die Absicht ein Buch zu schreiben und habe sie eigentlich immer noch nicht. Die meisten Themen (dieses hier eingeschlossen) wurden auf meinem Smartphone geschrieben. Während eines Fluges, im Zug oder in einem Café. Viele sind schnelle Beobachtungen, die sich aus meinen fundierten Kenntnissen des Bitcoin-Core-Codes oder dem langen Selbststudium und der Erfahrung in verschiedenen Disziplinen ergeben.

Mit der Zeit begannen die verschiedenen Themen miteinander zu interagieren, eine notwendige Taxonomie entstand und was zunächst ein gelegentlicher Prozess der Ad-hoc-Beobachtung war, wurde zu Arbeit. **Die Themen sind so kurz wie möglich und setzen ein gewisses Verständnis von Bitcoin und Ökonomie voraus.** Ich habe mir Mühe gegeben Beziehungen und Terminologie zu rationalisieren, mein Fokus lag allerdings auf Konsistenz[2] und der Erweiterung des Verständnisses. Glücklicherweise sind andere gekommen, um bei Illustration, Rezension und Veröffentlichung zu helfen.

Ich habe die Begriffe Katallaktik[3] und Praxeologie[4] verwendet, um die zugrundeliegende Disziplin zu beschreiben. Manche verwenden auch den Begriff Österreichische Schule[5]. Ich finde das alles unbefriedigend, daher habe ich angefangen, die Disziplin als "Rationale Ökonomie" zu bezeichnen (nicht zu verwechseln mit Ökonomischem

Referenzen

[1] https://de.wikipedia.org/wiki/Twitter_Inc.

[2] https://de.wikipedia.org/wiki/Widerspruchsfreiheit

[3] https://de.wikipedia.org/wiki/Katallaktik

[4] https://de.wikipedia.org/wiki/Praxeologie_(Wirtschaftswissenschaft)

[5] https://de.wikipedia.org/wiki/Österreichische_Schule

Rationalismus[1]). Ein System, das ausschließlich auf deduktiven Schlussfolgerungen[2], einer Reihe von Axiomen[3] beruht.

Es war Mises[4], der ausdrücklich ein Wirtschaftssystem auf rationaler Grundlage einführte, jedoch durchdringt dessen Ansatz nicht die gesamte Österreichische Schule (die älter ist als Mises). Rothbard[5] fügt Mises Strenge und Klarheit hinzu und leitet einige wichtige neue Schlussfolgerungen ab. Dennoch begeht Mises (wie die meisten Menschen) substanzielle Fehler[6], die unglücklicherweise von Rothbard weitergetragen werden. Andere Fehler, die innerhalb der Österreichischen Schule häufig verbreitet werden, sind offensichtliche Fehlinterpretationen.

In jedem Fall, in dem Mises irrt, kritisiert er das staatliche Fiatgeld[7]. Anders ausgedrückt scheint es, als opferte er seine Objektivität für seine Leidenschaft. Dennoch offenbart sein rationales Verfahren diese Fehler, sofern es korrekt angewendet wird. Staatliches Geld verdient Kritik und Bitcoiner lassen kaum eine Gelegenheit aus, diese zu äußern. Allerdings bedarf es *akkurater* Kritik. Alles andere ist kontraproduktiv. Mit einer korrekten Analyse können spezifische relevante Marktkräfte identifiziert werden, sowohl im Monopol-Fiatgeld (z.B. US-Dollar) als auch im Markt-Fiatgeld (z.B. Bitcoin). Eine derartige sachgemäße Analyse kann die Verschwendung wertvollen Kapitals für irrationale Vorschläge[8] begrenzen.

Referenzen

[1] https://en.wikipedia.org/wiki/Economic_rationalism
[2] https://de.wikipedia.org/wiki/Deduktion
[3] https://de.wikipedia.org/wiki/Axiom
[4] https://de.wikipedia.org/wiki/Ludwig_von_Mises
[5] https://de.wikipedia.org/wiki/Murray_Rothbard
[6] Kapitel: Inflationsprinzip
[7] Kapitel: Taxonomie des Geldes
[8] Kapitel: Vollreservefehlschluss

Ein streng rationaler Prozess deckt nicht nur Fehler auf, er bringt auch neue und interessante Entdeckungen[1] und Vereinfachungen[2] hervor, nicht nur für Bitcoin, sondern auch in der Wirtschaftstheorie allgemein. Die Themen formen einen Graphen, über den keine Totalordnung angemessen erscheint. Das Inhaltsverzeichnis ist eine mangelhaft auferlegte Ordnung. Obwohl hier einige Versuche unternommen wurden, Fortschritte zu erzielen, so empfehle ich doch, die Themen so zu lesen, wie sie geschrieben wurden – zur Befriedigung der Neugier.

Referenzen

[1] Kapitel: Eigenschaft der Zensurresistenz

[2] Kapitel: Abschreibungsprinzip

EINLEITUNG

Einleitung

Sie glauben, dass sie etwas über Bitcoin und die Österreichische Schule[1] der Ökonomie wissen? Wenn ja, dann sind Sie vielleicht bereit für Kryptoökonomie. Dies ist kein Buch für die Uneingeweihten. Es ist keine Erzählung und ist frei von Meinungen. Der Inhalt hat eine hohe Dichte – er wiederholt sich nicht. Es ist kein Beitrag zur Echokammer, wird Ihnen weder zeigen, wie man ein Wallet aufsetzt, noch den zukünftigen Preis nennen oder Ihnen sagen, was Sie tun sollen.

Kryptoökonomie wendet rationale Wirtschaftsprinzipien auf Bitcoin an und zeigt Mängel und unnötige Komplexität, sowohl in den Prinzipien selbst als auch im allgemeinen Verständnis von Bitcoin. Es wird Ihr Verständnis von beidem verbessern. Bitcoin benötigt eine neue, strenge und umfassende Disziplin. **Darum geht es.**

Bitcoin ist etwas Neues. Es scheint sich jedem Verständnis zu entziehen. Gab es jemals ein Geld mit einer festen Menge? Gibt es einen anderen Fall, in dem die Produktionskosten direkt vom Produktpreis abhängen? Gibt es noch irgendetwas anderes mit einer wettbewerbsfähigen aber festen Transaktionsrate? Um über den Hype hinauszusehen, das Wertversprechen, das Sicherheitsmodell und das ökonomische Verhalten zu verstehen, ist dieses Buch womöglich Ihre einzige Quelle.

Bitcoin ist Wirtschaft, Technologie und Sicherheit. Ohne die Berücksichtigung all dieser Aspekte werden Fehler gemacht. Ökonomen, Technologen, Sicherheitsexperten und sogar Numerologen[2] haben versucht es zu erklären. Jeder bringt eine begrenzte Perspektive mit und berücksichtigt wesentliche Aspekte nicht. Der Autor sah sich selbst als besonders geeignet dazu an, diese verschiedenen Aspekte zu vereinen.

Referenzen

[1] https://de.wikipedia.org/wiki/Österreichische_Schule

[2] https://twitter.com/100trillionusd

Seine Arbeit begann mit einem Hardware-Wallet. Er verbrachte ein Jahr damit Angriffsvektoren zu analysieren, arbeitete mit Experten für Elektronikdesign, Hardware-Exploits und staatliche Überwachung zusammen. Er entschied sich für die Softwarebibliothek Libbitcoin[1], da Satoshis Prototyp nicht für die Entwicklung vorgesehen war und außerdem größtenteils von der Bitcoin Foundation[2], einem Unternehmenskonsortium, finanziert wurde. Später widmete er sich Libbitcoin und schrieb oder editierte letztendlich alle ca. 500.000 Zeilen Code. Wenige haben vergleichbare Erfahrung mit einem so umfassenden Bitcoin-Stack.

Als gefechtserfahrener Kampfpilot der U.S. Navy[3] erlebte er staatliche Bedrohungen. Er wurde ein hochqualifizierter Ausbilder des Strike-Fighter-Taktik[4]-Programms, wobei seine Hauptaufgabe in der Taktikanalyse und der Darstellung von Bedrohungen lag. Er beriet die Marine ebenfalls zum Strike-Fighter-Training-System[5]-Netzwerk, im Joint-Strike-Fighter-Programm[6], frühen GPS-Waffen[7] und F/A-18[8]-Systemen. Sein Verständnis der physischen Natur aller Sicherheit wurde durch jahrzehntelanges Training japanischer Kampfkünste gestärkt, durch das er in fünf Disziplinen den schwarzen Gürtel erreichte.

Seine universitäre Bildung[9] und seine Erfahrungen in der Informatik paarten sich mit umfangreicher Geschäftserfahrung, während er mehrere Unternehmen gründete. Er

Referenzen

[1] https://libbitcoin.info

[2] https://bitcoinfoundation.org

[3] https://www.navy.mil

[4] https://de.wikipedia.org/wiki/United_States_Navy_Fighter_Weapons_School

[5] https://www.globalsecurity.org/military/library/policy/navy/ntsp/SFTS.htm

[6] https://de.wikipedia.org/wiki/Joint-Strike-Fighter-Programm

[7] https://en.wikipedia.org/wiki/Guided_bomb#Satellite

[8] https://de.wikipedia.org/wiki/McDonnell_Douglas_F/A-18

[9] https://www.rpi.edu

arbeitete bei IBM[1] und als Principal Architect bei Microsoft[2], zwei der größten Unternehmen der Welt. Das letztere kaufte sein erstes Startup, sein zweites wurde von Veritas Capital[3] übernommen. In diesem Zusammenhang wurden ihm drei US-Patente[4] zugesprochen. Schließlich wurde er zu einem Business Angel, der seine Erfahrungen mit anderen Gründern teilt.

Als CTO[5] seiner ersten Firma veröffentlichte er drei Computersicherheitsrichtlinien durch das CERT Coordination Center[6]. Jede wurde ausschließlich aus seinem Studium der Benutzerdokumentation abgeleitet. Später erhielt er für seine Arbeit zum Software-Patching einen Sitz im Beirat der DHS[7] Open Vulnerability Assessment Language[8]. In den letzten Jahren deckte er erhebliche Sicherheitslücken in jeder der ersten drei Iterationen einer beliebten Secure-Element-Hardware-Wallet auf, erneut anhand der Durchsicht der Benutzerdokumentation.

Dreißig Jahre Selbststudium der freien Marktwirtschaft wurden durch ausgedehnte Reisen rund um die Welt verstärkt. Bei seinen Besuchen in über 80 Ländern kam er mit Menschen auf fünf verschiedenen Kontinenten zusammen. Immer noch oft unterwegs auf dem Motorrad, nur mit einer Umhängetasche ausgestattet, erlangt er ein tiefes Verständnis für die globalen wirtschaftlichen Realitäten. Von simbabwischen Devisenhändlern auf dem Schwarzmarkt über tansanische Kaffeepflücker, venezuelanische Flüchtlinge, mongolischen Hirten, okinawanische Jazzmusiker, laotische Mönche und viele andere – die Welt ist nicht so, wie sie oft dargestellt wird.

Referenzen

[1] https://ibm.com

[2] https://microsoft.com

[3] https://www.veritascapital.com

[4] https://www.uspto.gov

[5] https://de.wikipedia.org/wiki/Technischer_Direktor

[6] https://en.wikipedia.org/wiki/CERT_Coordination_Center

[7] https://dhs.gov

[8] https://github.com/CISecurity/OVALRepo

Die Fähigkeit, diese vielfältigen und relevanten Erfahrungen miteinander zu verbinden, führte zu Kryptoökonomie. Dies ist Ihre nächste Haltestelle.

SICHERHEITSMODELL

Widerstandsaxiom

In der modernen Logik ist ein Axiom[1] eine Prämisse. Es kann nicht bewiesen werden. Es ist eine Grundannahme, gegen die andere Dinge bewiesen werden können. So kann man in der Euklidischen Geometrie[2] z.B. nicht beweisen, dass sich parallele Linien niemals treffen. Sie definiert lediglich die jeweilige Geometrie.

Der Beweis von Aussagen über Bitcoin erfordert den Rückgriff auf axiomatische Systeme, insbesondere Mathematik[3], Wahrscheinlichkeit[4] and Katallaktik[5] und damit auf die Annahmen, auf denen sie beruhen. Allerdings stützt sich Bitcoin auch auf ein Axiom, das in diesen Systemen nicht zu finden ist.

Satoshi spielt in einer frühen Stellungname[6] darauf an:

> >Du wirst in der Kryptografie keine Lösung für politische Probleme finden.
>
> Ja, aber wir können eine große Schlacht im Wettrüsten gewinnen und so für mehrere Jahre einen neuen Raum für Frieden erlangen.
>
> Regierungen sind gut darin, zentral gesteuerten Netzwerken wie Napster die Köpfe abzuschneiden aber reine P2P-Netzwerke wie Gnutella und Tor scheinen sich zu behaupten.
>
> *Satoshi Donnerstag, 6. November 15:15:40 EST 2008*

Anders ausgedrückt besteht die Annahme, dass es einem System möglich ist, sich der staatlichen Kontrolle zu widersetzen. Dies wird nicht als Tatsache akzeptiert, sondern

Referenzen

[1] https://de.wikipedia.org/wiki/Axiom

[2] https://de.wikipedia.org/wiki/Euklidische_Geometrie

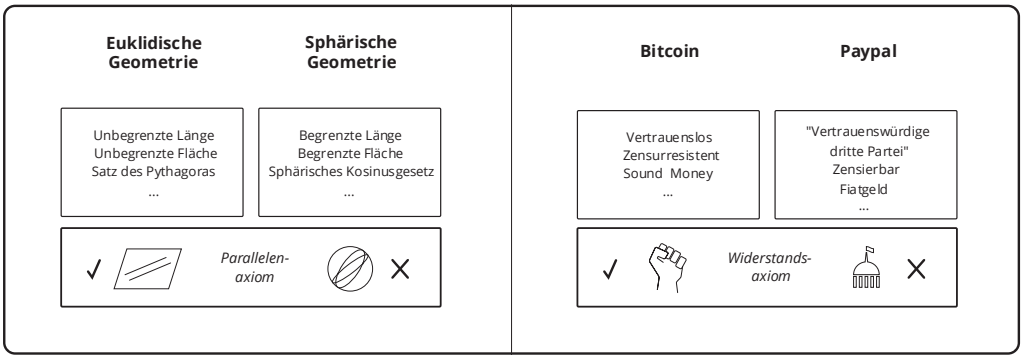
[3] https://de.wikipedia.org/wiki/Zermelo-Fraenkel-Mengenlehre

[4] https://en.wikipedia.org/wiki/Probability_axioms

[5] https://de.wikipedia.org/wiki/Katallaktik

[6] http://satoshi.nakamotoinstitute.org/emails/cryptography/4

aufgrund des Verhaltens ähnlicher Systeme als eine vernünftige Annahme angesehen, auf welcher das System basieren soll.



Wer das Widerstandsaxiom nicht akzeptiert, denkt über ein völlig anderes System als Bitcoin nach. Geht man davon aus, dass es einem System nicht möglich ist, staatlichen Kontrollen zu widerstehen, ergeben Schlussfolgerungen im Zusammenhang mit Bitcoin keinen Sinn – ebenso wie Schlussfolgerungen in der sphärischen Geometrie[1] dem Euklidischen widersprechen. Wie kann Bitcoin ohne das Axiom erlaubnisfrei[2] oder zensurresistent[3] sein? Der Widerspruch führt dazu, dass man bei dem Versuch, den Konflikt zu rationalisieren, offensichtliche Fehler[4] begeht.

Es ist üblich, dass Menschen ein Bitcoin-ähnliches System, das das Widerstandsaxiom auslässt, zynisch als „nur ein weiteres PayPal“ bezeichnen, und das nicht ohne Grund. Confinity[5] versuchte ursprünglich ein System mit einem ähnlichen Wertversprechen[6]

Referenzen

[1] https://de.wikipedia.org/wiki/Sphärische_Geometrie

[2] Kapitel: Prinzip der Genehmigungsfreiheit

[3] Kapitel: Eigenschaft der Zensurresistenz

[4] Kapitel: Hearn-Fehler

[5] https://en.wikipedia.org/wiki/Confinity

[6] Kapitel: Wertversprechen

wie Bitcoin zu schaffen. Als das nicht gelang, verwarfen sie das Axiom und schufen das PayPal[1], das wir heute kennen.

Referenzen

[1] https://de.wikipedia.org/wiki/PayPal

Eigenschaft der Zensurresistenz

Widerstand gegen Zensur ist eine Folge von Transaktionsgebühren. Die Durchsetzung von Zensur ist nicht von der Durchsetzung eines Soft-Fork zu unterscheiden, in dem die Hash-Power-Mehrheit nicht-zensierende Blöcke ablehnt. Ohne eine solche Durchsetzung werden Transaktionen auf wirtschaftlich-rationaler Basis bestätigt, trotz individueller Subjektivität des Miners.

Ein Miner der Mehrheit ist finanziell profitabel. Daher fallen für die Anschaffung der Zensurmittel keine Kosten an. Da es sich beim Mining zwangsläufig um eine anonyme[1] Aufgabe handelt, ist es für jeden Akteur möglich, die Mehrheits-Hash-Power zu erwerben und einzusetzen und diese jederzeit zu kontrollieren. Wie im Proof-of-Work-Fehlschluss[2] gezeigt, können Hard-Forks nicht dazu verwendet werden, den Zensor selektiv zu vertreiben. Stattdessen beschleunigen Sie den Zusammenbruch des Coins.

Bei aktiver Zensur können Gebühren für Transaktionen ansteigen, die nicht bestätigt werden. Dieser Gebührenaufschlag schafft ein größeres Gewinnpotenzial für Miner, die zensierte Transaktionen bestätigen. Bei ausreichendem Niveau führt diese Möglichkeit zu zusätzlichem Wettbewerb und damit zu einer Erhöhung der Gesamt-Hash-Rate.

Wenn die steigende nicht-zensierende Hash-Power die des Zensors übersteigt, schlägt dessen Durchsetzung fehl. Der Zensor steht somit vor der Wahl, die Maßnahmen zu subventionieren oder den Aufwand aufzugeben. Lediglich der Staat kann den Betrieb dauerhaft subventionieren, da er Steuern erzwingen kann. Gleichzeitig profitiert er von der Aufrechterhaltung seines eigenen Währungssystems. **Um die Durchsetzung der**

Referenzen

[1] Kapitel: Risikoverteilungsprinzip

[2] Kapitel: Proof-of-Work-Fehlschluss

Zensur aufrechtzuerhalten, muss der Staat mindestens Steuern in Höhe des Gebührenaufschlags einnehmen.

Ein Coin ohne integrierte Gebühren würde entweder an einer Zensur scheitern oder einen Nebengebührenmarkt entwickeln. Wie in Nebengebührfehlschluss[1] gezeigt, ist es nicht notwendig, Gebühren zu integrieren, die Integration von Gebühren ist jedoch eine wichtige Anonymisierungstechnik. In beiden Fällen ergibt sich die Zensurresistenz nur aus dem Gebührenaufschlag. Der Subventionsanteil der Blockbelohnung trägt nicht zur Zensurresistenz bei, da der Zensor die gleichen Subventionen erhält wie andere Miner.

Es ist möglich, dass die Durchsetzung der Zensur zu einem Preisverfall führen könnte, was wiederum dazu führen würde, dass dem Zensor ein betrieblicher Verlust entsteht. In diesem Fall wurde jedoch das Ziel erreicht, da die Wirtschaft keine Möglichkeit hatte, der Zensur entgegenzuwirken. Dieser Zusammenbruch könnte zu vernachlässigbaren Kosten dadurch erreicht werden, dass einfach die Absicht zur Zensur demonstriert wird. Es ist auch möglich, dass ein zensierender Soft-Fork zu einer *Preiserhöhung* führen könnte, da das Weißmarktgeschäft die damit verbundene staatliche Genehmigung annimmt. Dennoch, damit der Coin überleben kann, muss seine Wirtschaft weiterhin einen Gebührenaufschlag erwirtschaften, der ausreicht, um die Zensur zu überwinden.

Es kann nicht gezeigt werden, dass die Wirtschaft genügend Gebühren erwirtschaftet, um einen Zensor zu überwältigen. Ebenso kann nicht gezeigt werden, dass ein Zensor bereit und in der Lage sein wird, den Betrieb in jeder beliebigen Höhe zu subventionieren. Es ist daher nicht möglich, Zensurresistenz nachzuweisen. Deshalb ist Widerstand gegen staatliche Kontrolle axiomatisch[2].

Referenzen

[1] Kapitel: Nebengebührfehlschluss

[2] Kapitel: Widerstandsaxiom

Zentralisierungsrisiko

Die Schwachpunkte[1] von Bitcoin resultieren aus Zentralisierung sowie Kartellierung (Pooling). Kräfte, die zu einem aggregierten Mining führen, nennt man Kartellierungsdruck[2]. Während die Kartellierung die Bestätigungssicherheit schwächt, schwächt die Zentralisierung die Sicherheit der Konsensregeln. Schwäche entsteht dadurch, dass es weniger Menschen gibt, mit denen man das Risiko teilen[3] kann.

Das Konsensrisiko teilen sich nur aktive Händler, da sie diejenigen sind, die die Möglichkeit haben, den Handel mit Eigentum gegen Einheiten zu verweigern, die ihren Regeln nicht entsprechen. Finanzielle Kräfte, die die Anzahl der Händler verringern, werden als Zentralisierungsdruck bezeichnet. Das Problem der Delegation ist, dass sie gewöhnlich mit einer Zentralisierung verbunden ist, wie es z.B. bei Web-Wallets[4] typisch ist. Das Wallet besitzt nicht nur die gespeicherten Einheiten sondern kontrolliert auch die Validierung der im Handel erhaltenen Einheiten. **Letzteres reduziert die Macht über die Konsensregeln auf eine Person für alle Wallets des Dienstes.**

Zentralisierungsdruck umfasst:

- Rabatt auf Benutzerunfreundlichkeit.
- Rabatt auf On-Chain-Buchungen.

Wenn der Tausch für den Kunden schwierig ist, muss der Händler die Ware rabattieren, damit der Coin akzeptiert wird. Wenn der Tausch für den Händler schwierig ist, fallen zusätzliche Kosten an. Wenn Zahlungen an einen vertrauenswürdigen Dritten

Referenzen

[1] Kapitel: Qualitatives Sicherheitsmodell
[2] Kapitel: Risiko des Kartellierungsdrucks
[3] Kapitel: Risikoverteilungsprinzip
[4] https://bitcoin.org/de/wallets/web/

weitergeleitet werden, verringert sich die Höhe dieses Rabatts und/oder dieser Kosten und die Kapitalrendite erhöht sich.

Bei Überweisungen fallen Gebühren an, was einen Händler ebenfalls dazu auffordert, seine Ware zu rabattieren. Durch die Nutzung eines vertrauenswürdigen Vermittlers zur Abwicklung von Off-Chain-Überweisungen verringern sich seine Gebühren und folglich der Rabatt, was die Kapitalrendite des Händlers erhöht.

Zentralisierung manifestiert sich als:

- Zahlungsabwickler
- Web- und andere vertrauenswürdige Wallets
- Gehostete APIs zum Zugriff auf die Blockchain

In einem Umfeld mit geringer Bedrohung[1] hat der Händler den finanziellen Anreiz verringert, für die Bitcoin-Sicherheit zu bezahlen. Da die Kosten für Alternativen[2] steigen, wird der Rabatt unvermeidbar. An diesem Punkt entscheidet sich der Kunde, einen höheren Preis zu zahlen, oder der Händler schließt sein Geschäft, da das Kapital nach marktüblichen Renditen sucht.

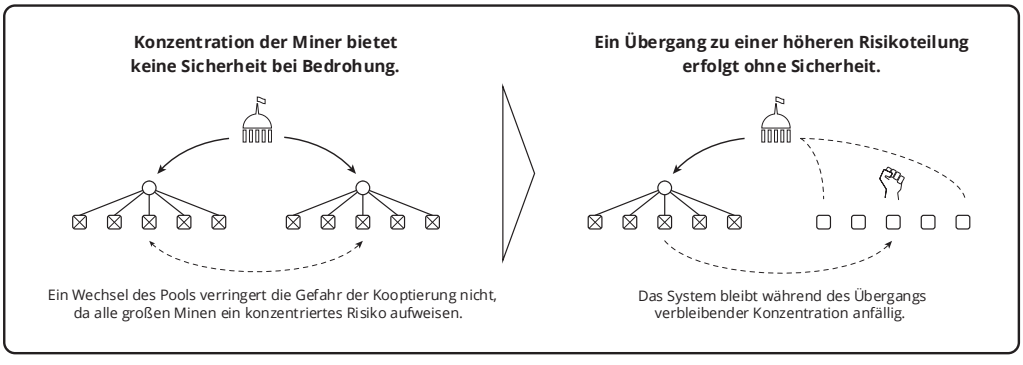
Referenzen

[1] Kapitel: Gefährdungsstufenparadoxon

[2] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

Kakerlakenfehlschluss

Es gibt eine Theorie, dass Aggregation die durch die Risikoverteilung[1] gebotene Sicherheit nicht wesentlich reduziert, da Miner und Wirtschaft sich bei Bedarf zerstreuen, ähnlich wie sich Kakerlaken zerstreuen, die vom Licht gestört werden. **Die Theorie impliziert irrationalerweise, dass Sicherheit tatsächlich existiert, weil sie existieren könnte.** Das ist im Wesentlichen eine Ablehnung des Gefährdungsstufenparadoxons[2], das impliziert, dass sich die Sicherheit im Laufe der Zeit unter einer anhaltenden Bedrohung weiterentwickelt.



Die Theorie basiert darauf, dass Grinder in die Gefolgschaft eines anderen Miners wechseln. Dies basiert auf dem Fehlschluss des Kräftegleichgewichts[3], welcher Miner fälschlicherweise als Bedrohung einstuft. Eine Verlagerung der Hash-Power von einer Mine zu einer anderen verringert weder die Kartellierung noch das damit verbundene Risiko[4]. Das Risiko besteht darin, dass Staaten große Mengen an Hash-Power

Referenzen

[1] Kapitel: Risikoverteilungsprinzip

[2] Kapitel: Gefährdungsstufenparadoxon

[3] Kapitel: Fehlschluss des Kräftegleichgewichts

[4] Kapitel: Risiko des Kartellierungsdrucks

übernehmen und so die Angriffskosten erheblich senken. Es ist ein Fehler anzunehmen, dass Staaten zur Verteidigung der Seigniorage[1] nicht zusammenarbeiten[2].

> Der Internationale Währungsfonds (IWF) ist eine Organisation von 189 Ländern, die sich für die Förderung der globalen Währungskooperation einsetzt...
>
> *imf.org*

Daher kann man nicht davon ausgehen, dass eine große Mine außerhalb staatlicher Kontrolle[3] existieren kann. Eine Verringerung der Kartellierung erfordert eine Erhöhung der Zahl der Miner, insbesondere derjenigen, die bereit und in der Lage sind, verdeckt[4] zu operieren. Dies erfordert, dass Grinder mit den höheren Kosten zu kämpfen haben, die mit einer geringeren Kartellierung einhergehen.

Dennoch kann man von den Menschen nicht erwarten, gegen ihre eigenen finanziellen Interessen zu arbeiten. Um die Risikoverteilung zu erhöhen, muss der finanzielle Druck gegen sie umgekehrt werden. Eine gegenteilige Annahme ist wirtschaftlich irrational.

Die Theorie ignoriert weiterhin die wirtschaftliche Zentralisierung und Delegation. Es ist ein Fehler anzunehmen, dass sich die Wirtschaft schnell dezentralisieren lässt, und eine Entdelegation wäre im Falle staatlicher Angriffe höchstwahrscheinlich nicht durchführbar, da Devisenverkehrsbeschränkungen[5] den Transfer üblicherweise einschränken.

Referenzen

[1] https://de.wikipedia.org/wiki/Seigniorage

[2] https://www.imf.org/en/home

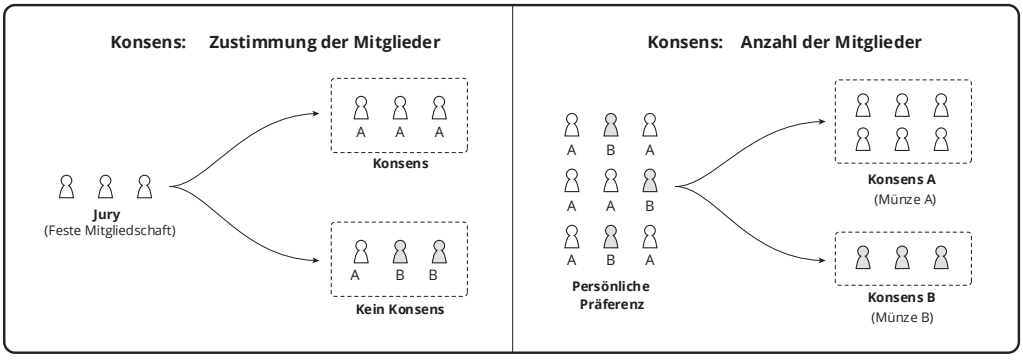
[3] Kapitel: Gefährdungsstufenparadoxon

[4] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/

[5] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

Konsenseigenschaft

Beim Thema Konsens denken Menschen häufig im Rahmen einer festen Mitgliedschaft, wie z.B. bei einer Jury[1]. In diesem Modell bedeutet Konsens, dass alle Mitglieder zustimmen müssen. **Da die Bitcoin-Mitgliedschaft jedoch erlaubnisfrei und daher nicht festgelegt ist, besteht immer eine vollständige Zustimmung, die durch die Mitgliedschaft impliziert wird.** In diesem Modell bezieht sich Konsens auf die Anzahl der Mitglieder (Größe der Wirtschaft) und nicht auf eine Bedingung für die Zustimmung.



Ein Konsens kann fragmentieren[2] oder sich festigen[3]. Im Allgemeinen bietet ein größerer Konsens einen größeren Nutzen und eine höhere Sicherheit durch eine breitere Risikostreuung[4].

Referenzen

[1] https://en.wikipedia.org/wiki/Hung_jury

[2] Kapitel: Fragmentierungsprinzip

[3] Kapitel: Konsolidierungsprinzip

[4] Kapitel: Risikoverteilungsprinzip

Kryptodynamische Prinzipien

Kryptodynamik ist ein Begriff, der hier geprägt wurde, um die Grundprinzipien von Bitcoin einfach zu beschreiben. Dies soll sowohl dem Verständnis von Bitcoin dienen, als auch dazu, es von anderen Technologien abgrenzen zu können. Die Prinzipien sind die minimale Teilmenge der kryptoökonomischen Prinzipien, die zum Erreichen dieses Ziels erforderlich sind.

Obwohl die Wahl des Namens nicht allzu wichtig ist, wird im Folgenden eine Begründung dafür gegeben.

Krypto[1]

> "Eine Kryptowährung ist ein [Geld], das starke Kryptographie verwendet, um Finanztransaktionen zu sichern, die Schaffung zusätzlicher Einheiten zu kontrollieren und die Übertragung von [Einheiten] zu überprüfen."
>
> *Wikipedia*

Dynamik[2]

> "Dynamik ist der Zweig der angewandten Mathematik, der sich mit der Untersuchung von Kräften [...] und ihrer Wirkung auf die Bewegung befasst."
>
> *Wikipedia*

Referenzen

[1] https://de.wikipedia.org/wiki/Kryptowährung

[2] https://de.wikipedia.org/wiki/Dynamik_(Physik)

Krypto + Dynamik

Kryptodynamik ist die Gesamtheit der Kräfte, die Bitcoin Transaktionen sichern, indem sie (1) die Definition von Einheiten und (2) den Transfer von Einheiten steuern.

Prinzipien

Sicherheitskräfte sind vollkommen menschlicher Natur. Menschen müssen handeln, um alles Mögliche abzusichern, auch Bitcoin. Als ein wirtschaftlich arbeitendes System kann die Bitcoin-Sicherheit nur davon ausgehen, dass Menschen in wirtschaftlich rationaler Weise handeln (Eigeninteresse). Daher basieren die Bitcoin-Sicherheitskräfte vollständig auf den eigennützigen Handlungen einzelner Personen, im Einzelnen:

- Risikoverteilung[1]
- Energieabfuhr[2]
- Machtregulierung[3]

Diese Kräfte hängen in ihrer Reihenfolge voneinander ab. Ohne Risikoteilung kann keine Energie in das System gesteckt werden, um die Macht eines Zensors zu regulieren. Wenn diese drei Kräfte intakt sind, kann Bitcoin sicher sein. Ohne jede einzelne von ihnen ist eine Technologie nicht Bitcoin.

Es kann nicht davon ausgegangen werden[4], dass eine Bitcoin-Implementierung unter Einbeziehung dieser Kräfte absicherbar ist. Darüber hinaus könnte eine besser

Referenzen

[1] Kapitel: Risikoverteilungsprinzip
[2] Kapitel: Proof-of-Stake-Fehlschluss
[3] Kapitel: Eigenschaft der Zensurresistenz
[4] Kapitel: Widerstandsaxiom

absicherbar sein als eine andere. **Es ist nur so, dass eine Technologie unter Einbeziehung dieser Kräfte ein Bitcoin ist und ohne sie nicht.**

Die durch diese Kräfte gebotene Sicherungsmöglichkeit kann als „kryptodynamische Sicherheit“ bezeichnet werden. So verstößt beispielsweise eine “genehmigungspflichtige Blockchain” gegen das Risikoverteilungsprinzip, eine strikte Proof-of-Stake-Technologie gegen das Prinzip der Energieabfuhr, und ein Geld, das vollständig auf Subventionen zur Entschädigung für Bestätigung angewiesen ist, verstößt gegen das Prinzip der Machtregulierung. Nichts davon ist kryptodynamisch sicher.

Prinzip des Verwahrungsrisikos

Wenn ein Vertrag einen Vermögenswert darstellt, stellt der Vertrag eine Forderung gegenüber dem Verwahrer des Vermögenswertes dar. Dieser Anspruch wird oft als Wertpapier (engl. Security) bezeichnet, mit der beabsichtigten Implikation, dass der Anspruch gegen das Versäumnis des Verwahrers, den Vermögenswert gemäß den Vertragsbedingungen umzutauschen, „abgesichert" ist. Der Geldwert des Wertpapiers entspricht dem des zugrundeliegenden Vermögenswerts abzüglich der Umtausch- und Durchsetzungskosten.

Das Verwahrungsrisiko ist ein zentraler Aspekt jedes Geldes[1]. Der Nutzen eines Geldes wird durch die Zuverlässigkeit seines Verwahrers begrenzt. Da es sich um einen Menschen handelt, kann die Zuverlässigkeit eines Verwahrers nicht gewährleistet werden. Im Falle von staatlichem Geld ist der Staat der alleinige Verwahrer. Wie im Reserveprinzip[2] gezeigt, dient Staatsgeld der Bildung einer Reserve[3]. Dies bringt dem Staat nur deshalb einen Vorteil, weil seine Verwahrungsfunktion sowohl durch die Auflösung der Reserve als auch durch die Ausgabe betrügerischer Wertpapiere außer Kraft gesetzt werden kann. Mit anderen Worten, der Verwahrungsausfall ist der Grund für staatliche Gelder.

Der Geldwert einer Bitcoin-Einheit hängt ausschließlich davon ab, was sie im Handel erwerben kann. Wenn kein Händler sie akzeptiert, ist eine Einheit für ihren Eigentümer nicht nützlich. Bitcoin benötigt keinen externen Verwahrer, aber im Interesse der Etablierung eines allgemeinen Prinzips, kann man die Gruppe aller Händler als

Referenzen

[1] Kapitel: Taxonomie des Geldes

[2] Kapitel: Reserveprinzip

[3] Kapitel: Definition der Reserve

kollektiven Bitcoin-Verwahrer betrachten. Somit verteilt sich das Verwahrungsrisiko auf die gesamte Wirtschaft.

Im Falle von Bitcoin bieten Händler ihr eigenes Eigentum im Austausch gegen das Geld an. Daher existiert keine implizite Verbriefung des Eigentums. Ein Händler kann die Annahme eines jeden Geldes beenden, was den Nutzen dieses Geldes verringert. Dies kann als Verwahrungsrisiko, nicht aber als Ausfall angesehen werden, da der Händler sich nicht verpflichtet hat, gegen das Geld Handel zu treiben. Wie im Fragmentierungsprinzip[1] gezeigt, liegt die Natur eines Splits im Wandel der Händlerakzeptanz.

Wie im Blockchain-Fehlschluss[2] gezeigt, kann die "Blockchain-Technologie" keinen Schutz vor dem Ausfall von Verwahrern bieten. Ein "tokenisierter" Vermögenswert ist ein Wertpapier. Die Möglichkeit von Betrug oder Diebstahl durch den Verwahrer, sei es direkt oder durch staatliche Anordnung, wird nicht verringert. **Genau wie bei Rohstoffgeldern wie Gold ist die Reduzierung des Verwahrungsrisikos, die Bitcoin bietet, keine Folge der Technologie oder vertraglichen Verpflichtungen, sondern der Größe seiner Wirtschaft.** Ironischerweise ist es die „Sicherheit", die unsicher ist.

Referenzen

[1] Kapitel: Fragmentierungsprinzip

[2] Kapitel: Blockchain-Fehlschluss

Hearn-Fehler

Es gibt eine Theorie, dass ein Staat beliebte Dinge nicht verbieten kann.

Dies impliziert, dass ein hoher Transaktionsdurchsatz eine wirksame Abwehr von Angriffen und Zwang ermöglicht. Dies wiederum impliziert, dass Bitcoin allein dadurch gesichert werden kann, dass man die zentralisierende Kraft eines sehr hohen Transaktionsdurchsatzes akzeptiert.

Die Theorie ist ungültig, da sie auf empirischen Beobachtungen basiert, sich jedoch auf einen faktischen Fehler stützt. **Es ist offensichtlich, dass Staaten es tatsächlich vorziehen, beliebte Dinge zu verbieten.** Im Folgenden finden Sie eine kurze Liste häufig verbotener beliebter Dinge:

- Drogen
- Glücksspiel
- Prostitution
- Religion
- Rede
- Versammlungen
- Handel
- Migration
- Waffen
- Arbeit
- Bücher
- Geld

Dieser Fehler kann dadurch entstehen, dass das Axiom des Widerstands[1] nicht akzeptiert wird, während weiter mit Bitcoin gearbeitet wird. Dies führt wahrscheinlich zu kognitiver Dissonanz[2]. Die anschließende Suche nach Erleichterung könnte einen hierherführen. Irgendwann jedoch ist der Fehler nicht mehr zu leugnen, was zu einem Wutausstieg[3] führen kann.

Referenzen

[1] Kapitel: Widerstandsaxiom

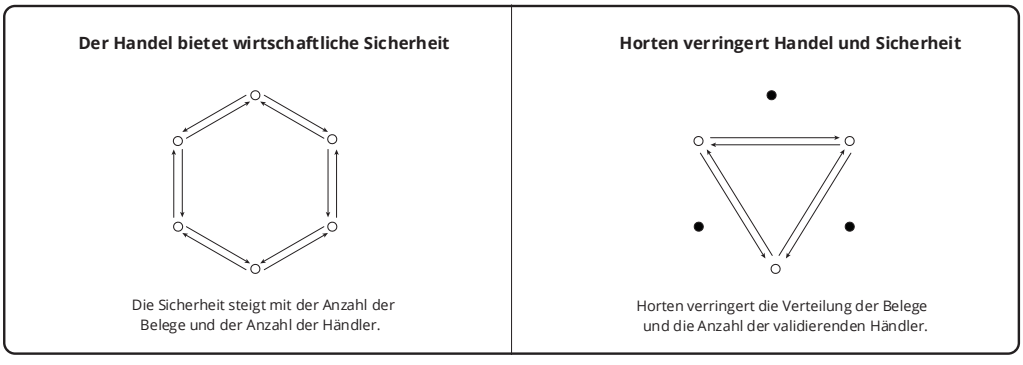
[2] https://de.wikipedia.org/wiki/Kognitive_Dissonanz

[3] https://en.wikipedia.org/wiki/Wikipedia:Rage_quit

Hortungsfehlschluss

Es gibt eine Theorie, dass vermehrtes Horten zu einem höheren Sicherheitsniveau eines Coins führt. Das ähnelt dem Dumping-Fehlschluss[1], basiert jedoch nicht unbedingt auf einer Spaltung.

Der vermeintliche Sicherheitsvorteil eines erhöhten Hortungsniveaus beruht auf der Theorie, dass ein Eigentümer ein Mitspracherecht bei der Validierung hat und die Wirtschaft daran hindern könnte, das zu akzeptieren, was die Eigentümer kollektiv als ungültiges Geld betrachten. Eigentümer handeln jedoch nicht, es sei denn, sie tauschen Einheiten gegen etwas ein, und in diesem Fall ist es der Händler, der die Konsensregeln durchsetzt. **Die Möglichkeit, dass Eigentümer gemeinsam handeln könnten, erhöht dieses Null-Kontrollniveau nicht. Die Theorie ist daher ungültig.**



Eine Steigerung kann nur relativ zu einem bestimmten Basisniveau beschrieben werden. Wenn eine Person davon überzeugt werden kann, dass ein höheres kollektives Horten die Systemsicherheit erhöht, dann besagt die Theorie, dass diese Person sich entscheiden kann, mehr zu horten, als andernfalls optimal wäre (d. h. das Basisniveau der Person). Dies läuft auf tatsächliche individuelle Kosten mit einem angenommenen

Referenzen

[1] Kapitel: Dumping-Fehlschluss

gesellschaftlichen Nutzen hinaus. Mit anderen Worten, die Theorie beruht auf irrationalem ökonomischem Verhalten, selbst wenn der Sicherheitsnutzen tatsächlich gegeben ist, und ist daher ungültig.

Die Theorie impliziert, dass weniger Handel mit dem Coin zu mehr Sicherheit führt. Das Gegenteil ist jedoch der Fall. Wie in Qualitatives Sicherheitsmodell[1] gezeigt, erfordert die Durchsetzung von Konsensregeln einen fortlaufenden Handel. Der Preis einer Einheit des Coins in einem anderen Gut[2] oder Geld ist willkürlich, steigt jedoch vorübergehend, wenn Einzelpersonen davon überzeugt werden, sich auf den Trugschluss zu verlassen. Der Nutzen dieser Erhöhung kommt den bestehenden Eigentümern zugute. Die Theorie, dass der Preis nur steigen kann, ist ein damit verbundener Spekulationsfehler, der im Mondfehlschluss[3] untersucht wird. Selbst ein nachweisbarer dauerhafter allgemeiner Preisanstieg würde diese Theorie nicht bestätigen, da sie sich nur auf eine vorübergehende relative Erhöhung bezieht, die durch finanziell suboptimale Einzelentscheidungen verursacht wird.

Referenzen

[1] Kapitel: Qualitatives Sicherheitsmodell

[2] Kapitel: Inflationsprinzip

[3] Kapitel: Mondfehlschluss

Fehlschluss der gerichtlichen Arbitrage

Es gibt eine Theorie, dass, da es unwahrscheinlich ist, dass sich alle Staaten einem Bitcoinverbot anschließen würden, der Coin dadurch überlebt, dass Mining und andere Aktivitäten in freizügigere Staaten abwandern.

Wer sich nicht daran hält, agiert aus Sicht der verbietenden Autorität im Schwarzmarkt[1]. Ein anderer Staat, der gegen ein Verbot verstößt, gilt aus dieser Perspektive als Schurkenstaat[2]. Ein Verbot ist eine einfache politische Aktion, gegen die Bitcoin keinen Schutz bietet.

Es gibt einen damit verwandten Fehlschluss[3], dass eine solche Maßnahme unmöglich schwierig wäre, wenn Bitcoin beliebt ist. Dahinter steckt die Idee, dass Bitcoin durch die Wahl abgesichert ist, was sein Sicherheitsmodell auf den Status quo von Staatsgeld reduziert und Bitcoins Wertversprechen[4] eliminiert.

Der Betrieb auf dem Weißmarkt wird durch ein Verbot per Definition eliminiert. Die Theorie impliziert daher, dass Bitcoin schließlich durch den Schutz von Schurkenstaaten gesichert ist. Dies reduziert sich auch auf die Sicherheit durch Abstimmung. Darüber hinaus verfügen mächtige Staaten über viele Instrumente[5], um andere zu nötigen, alles bis hin zu und einschließlich offenem Krieg. Diese Instrumente werden häufig in verschiedenen Kriegen eingesetzt, beispielsweise gegen Drogen, Geldwäsche und Terror. Ein Bitcoin-Verbot könnte problemlos unter den Rechtfertigungsvorwand all dieser bestehenden internationalen Konflikte fallen.

Referenzen

[1] https://de.wikipedia.org/wiki/Schwarzmarkt

[2] https://de.wikipedia.org/wiki/Schurkenstaat

[3] Kapitel: Hearn-Fehler

[4] Kapitel: Wertversprechen

[5] https://en.wikipedia.org/wiki/United_States_sanctions

Bitcoin ist jedoch speziell dafür konzipiert, ohne staatliche Genehmigung operieren zu können. Sein fortgesetzter Einsatz als Schwarzmarktwährung kann einen oder mehrere Staaten dazu veranlassen, seine Unterdrückung durch Zensur[1] zu versuchen. Auch wenn dies von einem einzelnen Staat versucht werden kann, ist es üblich, dass Staaten bei der Verteidigung der Besteuerungsmacht[2] ihrer Gelder zusammenarbeiten. Dies ist das Ziel des Internationalen Währungsfonds[3].

Eine solche Aktion kann am effizientesten[4] von einem einzigen geografischen Standort ausgeführt werden. In diesem Szenario bieten Schurkenstaaten keine Verteidigung, außer insoweit, als dass sie nicht nur bereit sind, auf den Steuervorteil ihres eigenen Geldes zu verzichten, sondern auch Steuergelder aufzuwenden, um der Zensur zu widerstehen. **Es kann nicht davon ausgegangen werden, dass Schurkenstaaten die Zensurbehörde überwältigen können, und jegliche Abhängigkeit von ihnen reduziert Bitcoin auf ein politisch gesichertes Geld.** Daher ist die Theorie ungültig.

Referenzen

[1] Kapitel: Prinzip der anderen Mittel

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] https://www.imf.org/en/Home

[4] Kapitel: Risiko des Kartellierungsdrucks

Prinzip der anderen Mittel

Bitcoin ist ein Akt des Widerstands[1], ein Versuch, „ein neues Territorium der Freiheit zu gewinnen“. Die Freiheit wird durch den ständigen Druck der Zwangsfinanzierung des Staates eingeschränkt. Es ist üblich, dass die Freiheit durch Blutvergießen erkämpft wird, mit dem konkreten Ziel, die Macht des Staates zu verringern. Bitcoin kann die Notwendigkeit des persönlichen Risikos bei der Erreichung dieses Ziels nicht beseitigen. Durch Risikoteilung[2] kann er die Inflationssteuer[3] jedoch möglicherweise ohne Blutvergießen senken. Dies wird Steuern nicht generell abschaffen, aber es könnte die Macht des Staates verringern, indem die Steuern deutlich sichtbarer werden.

Dieser Konflikt zwischen Staat und Individuen um die Kontrolle des Geldes[4] wird bis zu vier Phasen durchlaufen, wie sie das Bitcoin-Sicherheitsmodell[5] annimmt. Diese können sich überschneiden und regional unterschiedlich sein, sind aber alle klar erkennbar.

1. Flitterwochen
2. Schwarzmarkt
3. Wettbewerb
4. Kapitulation

Referenzen

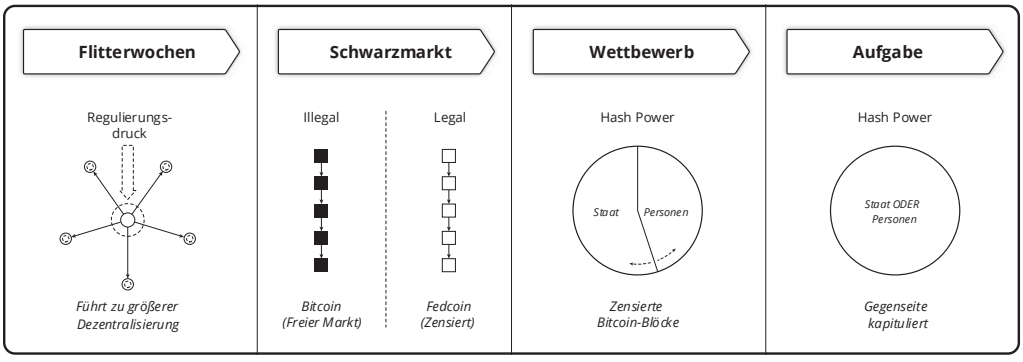
[1] Kapitel: Widerstandsaxiom

[2] Kapitel: Risikoverteilungsprinzip

[3] https://de.wikipedia.org/wiki/Seigniorage

[4] Kapitel: Taxonomie des Geldes

[5] Kapitel: Qualitatives Sicherheitsmodell



Die Flitterwochenphase ist gekennzeichnet durch den Wunsch staatlicher Stellen, die regulatorische Kontrolle über den Geld- und Wertpapierverkehr zu behalten. Zu diesem Zweck wird Druck auf die Aggregationspunkte ausgeübt. Wenn der Druck auf zusammengefasste Miner und zentralisierte Händler zunimmt, steigen die Kosten und der Nutzen sinkt. Um diese Kosten zu vermeiden, wird das Geld dann zwangsläufig stärker verteilt.

Wenn sich herausstellt, dass die Kontrollen an den Aggregationspunkten nicht ausreichen und das Bewusstsein wächst, dass die Seigniorage[1] in Gefahr ist, werden Transaktionen und das ergänzende Mining von Bitcoin verboten[2]. Da die Staaten zusammenarbeiten, um ihr Geld zu schützen, könnte sich daraus ein globaler „Krieg gegen Bitcoin“ entwickeln. Dies könnte mit der Einführung einer neuen offiziellen Währung einhergehen, z. B. Fedcoin[3]. Ziel wäre es, den Anschein zu erwecken, eine „sicherere“ Währung als Bitcoin einzuführen, während die Seigniorage- und Überwachungsvorteile elektronischer staatlicher Geldersatzmittel erhalten bleiben.

Bei ausreichendem Widerstand bleibt Bitcoin unabhängig von Fedcoin als Schwarzmarktgeld bestehen. An diesem Punkt kommt der Staat zu dem Schluss, dass die

Referenzen

[1] https://de.wikipedia.org/wiki/Seigniorage

[2] Kapitel: Hearn-Fehler

[3] Kapitel: Ziele eines Fedcoin

einzige wirksame Taktik darin besteht, als Miner anzutreten. Da das Mining notwendigerweise anonym[1] ist, gibt es für die Wirtschaft keine Möglichkeit[2], die staatliche Beteiligung am Mining zu verhindern. Somit tritt Bitcoin in die Wettbewerbsphase[3] ein, in der der Staat den Versuch eines 51%-Angriffs unternimmt.

Abgesehen von der anhaltenden Durchsetzung der Schwarzmarktphase ist die Wettbewerbsphase durch einen friedlichen Hash-Power-Machtkampf zwischen Staat und Einzelpersonen gekennzeichnet. Der Staat operiert aufgrund der Ablehnung zensierter Transaktionen mit Verlust. Dieser Verlust wird durch Steuereinnahmen ausgeglichen. Der Gebührendruck auf zensierte Transaktionen steigt[4] bis die staatliche Mining-Subvention durch dieses Gebührenniveau ausgeglichen wird. **An diesem Punkt steigen sowohl die Steuern als auch die Gebühren für zensierte Transaktionen, bis eine Seite des Konflikts kapituliert.**

Auf diese Weise kann Bitcoin möglicherweise einen Krieg mit anderen Mitteln[5] gewinnen. Es kann nicht davon ausgegangen werden, dass diese Kapitulation von Dauer sein wird. Wie das Gefährdungsstufenparadoxon[6] impliziert, wird das Geld wahrscheinlich in frühere Phasen abdriften, wenn die Bedrohung abnimmt.

Referenzen

[1] Kapitel: Prinzip der öffentlichen Daten
[2] Kapitel: Proof-of-Work-Fehlschluss
[3] Kapitel: Prinzip der anderen Mittel
[4] Kapitel: Eigenschaft der Zensurresistenz
[5] https://de.wikipedia.org/wiki/Carl_von_Clausewitz
[6] Kapitel: Gefährdungsstufenparadoxon

Patentwiderstandsprinzip

Im Gegensatz zum Urheberrecht ist das Patent eine marktfeindliche Kraft. Ein echtes Urheberrecht ist eine vertragliche Vereinbarung zwischen Käufer und Verkäufer, wohingegen ein Patent ausschließlich ein staatlich genehmigtes Monopol[1] darstellt. Das Patent ist kein „Angriff" des Patentinhabers, sondern ein verzerrender Kartellierungsdruck[2], verursacht durch den Staat.

Der Mining-Prozess ist sehr wettbewerbsintensiv. Monopolschutz bei der Verwendung effizienter Algorithmen[3] ist ein starker marktgegensätzlicher Zentralisierungsdruck. Bitcoin wird durch Menschen gesichert, die sich marktfeindlichen Kräften widersetzen[4]. Widerstand birgt ein größeres Risiko[5] wenn der Miner stark zentralisiert und/oder nicht anonym[6] ist.

Wenn sich die Menschen solchen Kräften nicht widersetzen, gibt es keine Sicherheit[7] im Geld. Mit zunehmender Bedrohungslage[8] werden die Folgen einer Patentverletzung ebenso risikoreich wie das Mining selbst. **Aus diesem Grund sind die Auswirkungen von Patenten nicht relevant, da sie die Sicherheit des Geldes betreffen.**

Referenzen

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/p/1075

[2] Kapitel: Risiko des Kartellierungsdrucks

[3] https://patents.google.com/patent/WO2015077378A1

[4] Kapitel: Widerstandsaxiom

[5] Kapitel: Risikoverteilungsprinzip

[6] Kapitel: Prinzip der öffentlichen Daten

[7] Kapitel: Qualitatives Sicherheitsmodell

[8] Kapitel: Gefährdungsstufenparadoxon

Prinzip der Genehmigungsfreiheit

Bitcoin ist so gestaltet[1], dass er ohne Genehmigung einer Behörde betrieben werden kann. Sein Wertversprechen[2] basiert vollständig auf dieser Eigenschaft.

Ein Markt kann aus Sicht des Staates in genehmigungspflichtige und genehmigungsfreie Märkte unterteilt werden Der Einfachheit halber wird ersterer oft als „weißer Markt" und letzterer als „schwarzer Markt" bezeichnet. Der Handel auf dem weißen Markt erfordert per Definition eine Erlaubnis, der auf dem Schwarzmarkt nicht.

Es ist eine einfache Definitionsfrage, **dass der Betrieb von Bitcoin nicht gleichzeitig auf dem weißen Markt stattfinden und genehmigungsfrei sein kann.** Jede Person, die auf dem weißen Markt tätig ist, benötigt dafür eine Genehmigung. Bitcoin ist daher von Natur aus ein Schwarzmarktgeld. Seine Sicherheitsarchitektur geht zwangsläufig davon aus, dass es ohne staatliche Genehmigung[3] operiert.

Die Sicherheit von Bitcoin erstreckt sich nicht auf Weißmarktsysteme. Jedes System, das vom Wertversprechen von Bitcoin abhängt, muss auch ein Schwarzmarktsystem sein.

Referenzen

[1] Kapitel: Kryptodynamische Prinzipien

[2] Kapitel: Wertversprechen

[3] Kapitel: Prinzip der anderen Mittel

Fehlschluss des Gefangenendilemmas

Es gibt eine Theorie, dass einzelne Staaten bei der Entscheidung, sich einem Verbot von Bitcoin anzuschließen, vor einem Gefangenendilemma[1] stehen. Ein sinnvolles Verbot impliziert, dass ein oder mehrere Staaten (das „Gefängnis“) wirtschaftliche Sanktionen[2] (zumindest) gegen andere Staaten (die „Gefangenen“) verhängen, die möglicherweise zu Bitcoin als Leitwährung[3] wechseln.

Wir gehen davon aus, dass die Gefangenen, die sich für die Verwendung von Bitcoin entscheiden, Handelspartner sind. Mit anderen Worten erfordert seine Verwendung als Reservewährung einen Partner, mit dem man Transaktionen abwickeln kann.

Der ordinale Nutzen[4] wird durch den subjektiven Wert[5] impliziert. Als Ergebnis werden keine Unentschieden[6] beobachtet, was ein starkes Dilemma impliziert. Sowohl symmetrische als auch asymmetrische Wissensannahmen werden ausgewertet.

Das Ergebnis für die individuelle Bitcoin-Einführung (Dummheit (Sucker, S)) :

- Wirtschaftliche Sanktion.
- Keine Handelspartner (die Dollar verwenden).
- Eine nicht nutzbare Reservewährung (keine Handelspartner).

Referenzen

[1] https://de.wikipedia.org/wiki/Gefangenendilemma

[2] https://www.cfr.org/backgrounder/what-are-economic-sanctions

[3] https://de.wikipedia.org/wiki/Leitwährung

[4] https://en.wikipedia.org/wiki/Ordinal_utility

[5] https://en.wikipedia.org/wiki/Subjective_theory_of_value

[6] https://de.wikipedia.org/wiki/Unentschieden

Das Ergebnis für eine gemeinsame Bitcoin-Einführung (Belohnung (Reward, R)) :

- Wirtschaftliche Sanktion
- Wirtschaftliche Sanktion gegen den Handelspartner.
- Eine Reservewährung, die nicht durch Seigniorage besteuert wird.

Das Ergebnis für die individuelle Einführung des Dollars (Versuchung (Temptation, T)) :

- Keine wirtschaftliche Sanktion.
- Wirtschaftliche Sanktion des Handelspartners.
- Eine Reservewährung, die durch Seigniorage besteuert wird.

Das Ergebnis für die gemeinsame Einführung des Dollars (Bestrafung (Punishment, P)) :

- Keine wirtschaftliche Sanktion.
- Keine wirtschaftliche Sanktion des Handelspartners.
- Eine Reservewährung, die durch Seigniorage besteuert wird.

Starkes symmetrisches Dilemma mit ordinalen Ergebnisbeziehungen

Brasilien\Irland	Bitcoin	Dollar
Bitcoin	R\R	S\T
Dollar	T\S	P\P

Um als Gefangenendilemma zu gelten, muss T > R > P > S wahr sein[1], wobei:

- T > R und P > S implizieren, dass der Dollar für beide die dominante Strategie ist.

Referenzen

[1] https://plato.stanford.edu/entries/prisoner-dilemma/#Symm2t2PDOrdiPayo

- R > P impliziert, dass beide den gemeinsamen Bitcoin dem gemeinsamen Dollar vorziehen.

Wir können schlussfolgern, dass P > S gilt, da individuelle Sanktionen keine internationale Einigung und daher keinen Nutzen aus einer Fremdwährungsreserve[1] bedeuten und Sanktionen vermutlich unerwünscht sind.

Um zu bestimmen, ob R > P und T > R gelten, ist eine objektive Methode erforderlich, die nur Seigniorage und Sanktionen in Beziehung setzt, da Sanktionen vermutlich unerwünscht sind. Dies kann man durch die Beobachtung erreichen, dass Gold weder Seigniorage[2] noch Sanktionen unterliegt. Anders gesagt bietet Gold die obigen Vorteile von Bitcoin ohne Sanktionen. Dennoch wurde Gold nicht ausgewählt (und wurde zuvor zugunsten des Dollars fallengelassen), was bedeutet, dass die Einführung des Dollars, der des Goldes und damit des Bitcoins vorzuziehen ist. Daher ist keine der Strategien[3] gültig. **Daher gibt es kein Dilemma.**

Starkes asymmetrisches Dilemma mit ordinalen Ergebnisbeziehungen

Brasilien\Irland	Bitcoin	Dollar
Bitcoin	Rr\Rc	Sr\Tc
Dollar	Tr\Sc	Pr\Pc

Um als Gefangennendilemma zu gelten, muss Ti > Ri > Pi > Si wahr sein[4], wobei:

- Tr > Rr und Pr > Sr

Referenzen

[1] https://de.wikipedia.org/wiki/Währungsreserve

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] https://de.wikipedia.org/wiki/Dominante_Strategie

[4] https://plato.stanford.edu/entries/prisoner-dilemma/#Asym

- Tc > Rc und Pc > Sc
- Rr > Pr und Rc > Pc

Wenn alle diese Beziehungen gelten, ist der individuelle Dollar dem Bitcoin vorzuziehen, und der gemeinsame Bitcoin ist vorzuziehen. Da dies die gleichen Beziehungen sind, die im symmetrischen Szenario ausgewertet werden, gibt es kein Dilemma.

Andere Annahmen

Die Gold-Bitcoin-Beziehung geht davon aus, dass die Clearing[1]-Kosten für den Transport von Gold und die Bestätigung von Bitcoin im Rahmen der internationalen Abwicklung vernachlässigbar[2] sind. Das Clearing erfordert lediglich die regelmäßige Verschiebung von Zahlungsungleichgewichten zwischen Staaten.

> ... jede Korrektur eines wirtschaftlichen Ungleichgewichts würde beschleunigt und es wäre im Normalfall nicht notwendig, zu warten, bis größere Mengen Gold von einem Land in ein anderes transportiert werden müssten.
>
> *gold.org*

Der Dollar wurde dem Gold vorgezogen, obwohl er ein ähnliches Gewicht hat, deutlich größer ist und der Seigniorage unterliegt. Die Beziehung zwischen Gold und Bitcoin geht davon aus, dass es keinen Unterschied in Volatilität und Liquidität gibt, obwohl Gold Bitcoin in beiden Bereichen objektiv übertrifft[3]. Da Gold und Bitcoin beide stabile Gelder[4] sind, wird für beide keine spekulative Rendite angenommen. Andere monetäre

Referenzen

[1] https://de.wikipedia.org/wiki/Clearing

[2] https://www.gold.org/history-gold/the-classical-gold-standard

[3] https://coinweek.com/bitcoin-vs-gold-10-crystal-clear-comparisons/

[4] Kapitel: Stabilitätseigenschaft

Eigenschaften von Gold, Bitcoin und Dollar werden als gleichwertig oder nicht relevant für staatliche Reservewährungen angesehen.

Fehlschluss der privaten Schlüssel

Private Schlüssel sichern nicht Bitcoin, sie sichern Einheiten von Bitcoin. **Die Kontrolle privater Schlüssel dient der individuellen Sicherheit, nicht der Systemsicherheit.** Wer auch immer die Schlüssel kontrolliert, ist der Eigentümer, und Bitcoin bietet diesem Eigentümer Sicherheit, selbst wenn die Schlüssel gestohlen werden. Eine dezentrale Validierung sichert den Konsens und eine verteilte Hash-Power-Mehrheit sichert die Bestätigung, aber die Sicherheit privater Schlüssel ist das Problem des Eigentümers.

Proof-of-Work-Fehlschluss

Händler kaufen Mining-Dienste, die ihren Regeln entsprechen, gegen eine zufriedenstellende Gebühr. Es gibt eine Theorie, dass Mining-Dienste in diesem Handel untergeordnet sind. Diese Unterordnung wird manchmal als „Asymmetrie“ oder „Benutzerherrschaft“ beschrieben. Diese Theorie lässt die Leute glauben, dass Mining stark kartelliert sein kann, solange die Händler nicht zentralisiert sind, da die Wirtschaft das Verhalten des Minings kontrollieren kann, was das System sicher macht. Die Konsequenz dieser ungültigen Theorie ist Selbstgefälligkeit in Bezug auf die durch Kartellierung verursachte Unsicherheit.

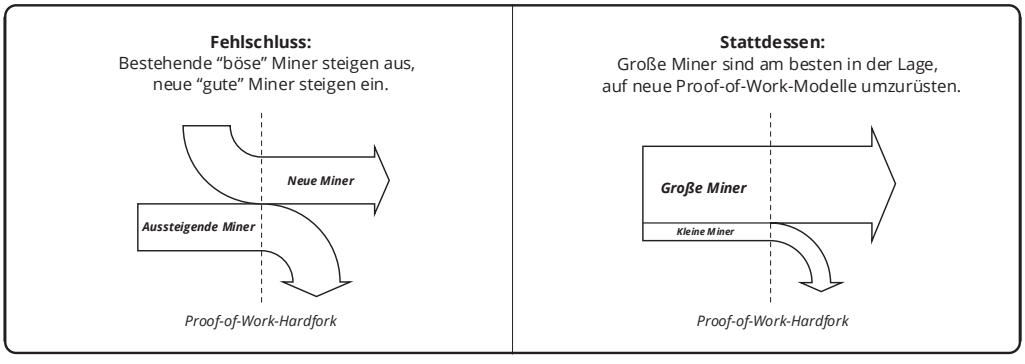
Miner kontrollieren die Transaktionsauswahl, während Händler das im Austausch angebotene Eigentum kontrollieren. Wenn ein Teil der Wirtschaft mit der Transaktionsauswahl der Miner unzufrieden ist, kann dieser sein Eigentum in Form eines abgespaltenen Coins mit einer anderen Arbeits-Regel zum Verkauf anbieten, die alle Grinding-Hardware überflüssig macht. Dies bezeichnet man typischerweise als Proof-of-Work-Hard-Fork.

Dieser Theorie zufolge erleiden die Miner dann einen katastrophalen Verlust aufgrund der nicht wieder einbringlichen Kapitalinvestition in hochspezialisierte Hardware. Der Hard-Fork kann eine Anpassung der Schwierigkeit umfassen, sodass die Bestätigung trotz eines vermutlich deutlichen Rückgangs der Hash-Rate fortgesetzt werden. Aufgrund der geringeren Schwierigkeit und des vermutlichen Mangels an spezialisierter Hardware können mehr Personen minen. Dies führt neue Miner in das Geschäft ein und reduziert die Kartellierung.

Es wurde gesagt, dass diese Fähigkeit der Wirtschaft, ihren Handelspartnern einen Kapitalverlust aufzuzwingen, eine einzigartige Asymmetrie im Vergleich zu anderen Märkten darstellt. Eine Gemeinschaft von Apfelkäufern kann beispielsweise nicht einfach die Obstgärten aller ihrer Lieferanten „zerstören“. **Die Theorie verkennt, dass es**

im Handel keine Asymmetrie gibt. Wenn alle Apfelkäufer beschließen, keine Äpfel von bestehenden Obstgärten zu kaufen, haben sie diese Macht sicherlich.

Ebenso haben die Obstplantagen die Möglichkeit, nicht zu verkaufen. Der Preis ist die kontinuierliche Lösung dieser Spannung. Dies ist genau die gleiche Dynamik, die auf jedem Markt existiert.



Die Theorie berücksichtigt auch nicht den Mangel an Identität. Sie geht davon aus, dass der Kapitalverlust den Ausstieg bestehender „schlechter" Miner und den Eintritt neuer „guter" Miner zur Folge haben wird. Diese Annahme ist nicht haltbar. Es gibt keinen Grund zu der Annahme, dass bestehende Miner aussteigen werden, und es gibt auch keinen Grund zu der Annahme, dass neue Miner nicht dieselben Entscheidungen treffen würden wie frühere Miner, da sie im selben Geschäft tätig sind, vorausgesetzt, man könnte den Unterschied überhaupt erkennen. Zumindest im Apfelszenario weiß man, von wem man Äpfel kauft und kann unterscheiden. Dies ist bei Bitcoin nicht möglich.

Die Theorie berücksichtigt ebenfalls nicht die Ökonomie des Minings. Die Nähe bietet einen Vorteil[1], der für Miner mit größerer Hash-Leistung zu höheren Kapitalrenditen führt. Größere Miner sind daher profitabler als kleine Miner. Größere Miner werden

Referenzen

[1] Kapitel: Fehler der Vorteile der Nähe

daher besser kapitalisiert sein als ihre kleinere Konkurrenz. Wenn die Regeländerung eintritt, werden diejenigen Miner übrigbleiben, die sich eine Umrüstung leisten können, und das werden die größten sein.

Es ist irrational anzunehmen, dass alle Miningunternehmen einfach aussteigen werden. Würden wir erwarten, dass alle Apfelbauern durch neue Apfelbauern ersetzt werden? Sind im Mining nicht Fachwissen, Einrichtungen, Energieverträge, Verfahren und nicht spezialisierte Maschinen wichtige Vorteile gegenüber Neulingen? Bestehende Miner haben einen inhärenten Vorteil gegenüber ihren vermeintlichen Nachfolgern. Das bedeutet, dass sie besseren Zugang zu Kapital haben. So haben nicht nur größere Miner weniger Konkurrenz, sondern alle verbleibenden bestehenden Miner haben einen Vorteil gegenüber allen neuen Minern.

Die Theorie berücksichtigt auch nicht, dass Händler Mining benötigen. Mining wird durch Splitting nicht ersetzt und behält die vollständige Kontrolle über die Transaktionsauswahl. Wenn es sich bei den „schlechten" Minern beispielsweise um Staaten handelt, welche den Coin angreifen, werden der Staat selbst und die kooptierten Miner mit derselben Störung weitermachen, bei geringeren Energiekosten. Wenn andere Miner aufgrund einer effektiven 100-prozentigen Steuer scheitern, sinken die Energiekosten des Angreifers weiter. Mining-Dienste, die für Händler „gut" sind, können nicht durch Splitting erbracht werden.

Schließlich berücksichtigt die Theorie keine Versicherungsfolgen. Basierend auf dem bisherigen Kapitalverlust, den alle Miner für einen bestimmten Coin erlitten haben, werden sich alle zukünftigen Miner seines Nachfolgers gegen die Wahrscheinlichkeit eines ähnlichen Ereignisses versichern. Sie können sich zwar selbst versichern, aber die erhöhten Kosten sind unvermeidlich. Dies wird die Hash-Rate bei gleicher Gebühr reduzieren, bis die Möglichkeit eines solchen Ereignisses als vernachlässigbar angesehen wird. Die Wirtschaft reduziert also ihre eigene Sicherheit vor Doppelausgaben und endet mit denselben Minern und einer größeren Kartellierung. Dies ist eine Verringerung der Sicherheit auf zwei Ebenen und ohne Nutzen.

Prinzip der öffentlichen Daten

Aus dem Risikoverteilungsprinzip[1] folgt, dass die Systemsicherheit von verdecktem Mining und Handel abhängt. Ein Coin existiert als ein gegenseitig vorteilhafter[2] Markt zwischen Minern und Händlern für die Bestätigung von Transaktionen innerhalb von Blöcken im Austausch gegen Gebühren.

Die notwendigerweise verdeckten Aktivitäten aufgelistet nach der Rolle des Urhebers:

Miner

- Blöcke erhalten [um darauf aufzubauen]
- Unbestätigte Transaktionen erhalten [um Gebühren zu verdienen]
- Blöcke erstellen und verteilen [um andere darauf aufbauen zu lassen]
- Zahlungen für Bestätigungen erhalten [um den Betrieb zu finanzieren]

Händler

- Blöcke erhalten [um Kundenzahlungen zu bestätigen]
- Unbestätigte Transaktionen erhalten (optional) [um Zahlungen und Gebühren vorherzusehen]
- Transaktionen erstellen und verteilen [um Kundenzahlungen zu erhalten]
- Zahlungen für Bestätigungen durchführen [um die Bestätigung zu kompensieren]

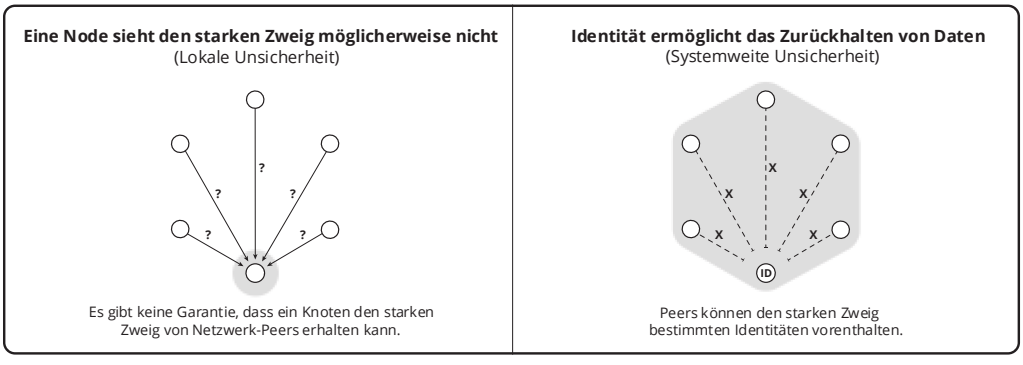
Wenn Blöcke nicht anonym abgerufen werden können, ist das System unsicher. Die Unfähigkeit, die stärksten Blöcke zu erhalten, die anderen Personen zur Verfügung

Referenzen

[1] Kapitel: Risikoverteilungsprinzip

[2] Kapitel: Fehlschluss des Kräftegleichgewichts

stehen, stellt eine Partitionierung des Netzwerks dar, die eine lokale Unsicherheit impliziert. Allerdings können weder Anonymität, noch ihr Gegenteil, die Identität, garantieren, dass man zu jedem gegebenen Zeitpunkt den stärksten Zweig sieht. Mit anderen Worten, jeder Versuch, die Partitionierung durch die Einführung von Identität abzumildern, ist eine falsche Entscheidung[1], durch die die Systemsicherheit dem falschen Versprechen einer lokalen Sicherheit geopfert wird.



Es ist nicht unbedingt erforderlich, dass alle Miner oder Händler alle Transaktionen zu einem bestimmten Zeitpunkt sehen. Eine umfassende Transparenz ist jedoch vorzuziehen, da sie den robustesten Wettbewerb um Gebühren und die besten führenden Informationen erzeugt. Mit anderen Worten, ein Markt, auf dem jeder Teilnehmer alle Transaktionen zu jeder Zeit sieht, ist ein perfekter Markt[2]. Das Netzwerk nach bestimmten Transaktionen zu fragen, anstatt nach allen (oder nach zusammenfassenden Informationen über alle), ist eine Quelle der Verfälschung und muss auch im Interesse der Sicherheit vermieden werden.

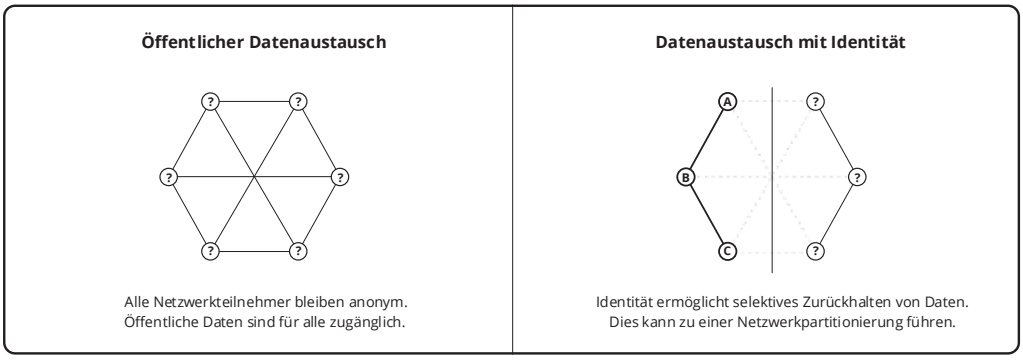
Die Erstellung von Blöcken und Transaktionen gibt die Identität nicht automatisch preis, die öffentliche Verbreitung dieser Informationen ist jedoch die Hauptquelle der

Referenzen

[1] https://de.wikipedia.org/wiki/Falsches_Dilemma

[2] https://de.wikipedia.org/wiki/Vollständige_Konkurrenz

Verunreinigung. Sofern sich Miner offen zu erkennen geben, gehen sie von einer Umgebung mit niedriger Bedrohungsstufe[1] aus und tragen nicht zur Systemsicherheit bei. Um bei der Verbreitung von Blöcken und Transaktionen eine Verfälschung zu vermeiden, ist eine anonyme Verbindung[2] zu einem Community-Server erforderlich. Dadurch wird sichergestellt, dass das Verteilungsnetzwerk niemals Zugriff auf identifizierende Informationen hat.



Proof-of-Work wahrt die Anonymität der Miner. Beim Mining ist keine Signatur erforderlich und Energie ist allgegenwärtig. Ebenso ist die Möglichkeit, anonym für die Bestätigung zu bezahlen, der Grund für die Einbeziehung von Transaktionsgebühren. Es ist ausreichend[3], einen Miner direkt (Off-Chain) für die Bestätigung zu bezahlen, jedoch enthüllt dies Händler und Miner gegenseitig und erschwert die anonyme Schätzung von Gebühren.

Bitcoin ist insofern neuartig, als dass alle Finanztransaktionen anhand öffentlicher Daten und ohne Identität validiert werden. Zentralisierte Finanzsysteme basieren entweder auf Vertrauen in (kryptografisch identifizierbare) Verbindungen zu anderen Parteien oder auf Vertrauen in (kryptografisch verifizierbare) Signaturen auf

Referenzen

[1] Kapitel: Gefährdungsstufenparadoxon

[2] https://de.wikipedia.org/wiki/Anonymizer

[3] Kapitel: Nebengebührfehlschluss

übertragenen Daten. Dies ist die Essenz vertrauensbasierter Systeme; bestimmte Autoritäten haben Geheimnisse, die andere verwenden, um deren Authentizität zu überprüfen. **Der Grund für Validierung besteht darin, die Verwendung von Identität und damit Autorität zu eliminieren.**

Qualitatives Sicherheitsmodell

Dezentralisierungsmodell

Im Prinzip des sozialen Netzwerks[1] wird gezeigt, dass Bitcoin ein Netzwerk menschlicher Beziehungen ist. Dies kann als gerichteter Graph[2] modelliert werden, bei dem jeder Knoten einen Händler und jede Kante einen Handel gegen Bitcoin darstellt. Kanten zeigen die Bewegungsrichtung des Coins an und werden in der Anzahl der gehandelten Einheiten quantifiziert. Es wird davon ausgegangen, dass alle Besitzer zum Zeitpunkt des Erhalts des Coins Händler waren, einschließlich der Miner (Verkauf von Bestätigungen) und als Empfänger von Charity (Verkauf von Goodwill[3]).

Wenn eine Person Coins nicht persönlich annimmt oder angenommene Coins nicht persönlich validiert, kann sie ungültige Coins nicht zurückweisen. Sie überträgt diese Aufgabe einer zentralen Autorität. **Alle Personen, die denselben Delegierten verwenden, werden auf nur einen Knoten reduziert, der den Delegierten darstellt.**

Für jeden Zeitraum ist die wirtschaftliche Sicherheit eine Funktion der Anzahl der Händler und der Ähnlichkeit der gehandelten Mengen. Die stärkste Wirtschaft bedeutete, dass alle Menschen auf der Welt in diesem Zeitraum die gleiche Anzahl von Einheiten handeln würden, ein Ideal, das man als „verteilte“ (oder vollständig dezentralisierte) Wirtschaft bezeichnen könnte. Die schwächste wäre, wenn ein einziger Delegierter alle in dem Zeitraum gehandelten Einheiten akzeptiert, was eine „zentralisierte“ Wirtschaft darstellen würde.

Referenzen

[1] Kapitel: Prinzip des sozialen Netzwerks

[2] https://de.wikipedia.org/wiki/Graph_(Graphentheorie)#Gerichteter_Graph_(Digraph)

[3] https://de.wikipedia.org/wiki/Geschäfts-_oder_Firmenwert

Genauer gesagt ist das System am wirtschaftlichsten dezentralisiert, welches die größte Anzahl von Knoten (Händlern) mit dem niedrigsten Variationskoeffizienten[1] in den eingehenden Kanten (Einnahmen) hat. Wenn wir eine Verteilungsfunktion als Umkehrung des Variationskoeffizienten definieren, erhalten wir:

```
Wirtschaftliche Dezentralisierung = Verteilung(Einnahme) * Händler
```

Ähnlich wie die wirtschaftliche Sicherheit kann die Bestätigungssicherheit als kantenloser Graph[2] modelliert werden. Jeder Miner wird durch einen Knoten im Graphen dargestellt. Ein Grinder ist kein Miner, da der Grinder keine Entscheidungsbefugnis hat, lediglich der Miner wird dargestellt. Die gesamte Hash-Power, die ein Miner einsetzt, ist das Gewicht des Knotens.

Für jeden Zeitraum ist die Bestätigungssicherheit eine Funktion der Anzahl der Miner und der Ähnlichkeit der von ihnen gesteuerten Hash-Power. Der stärkste Widerstand gegen Zensur wäre, wenn alle Menschen auf der Welt in diesem Zeitraum mit der gleichen Hash-Leistung minen würden, ein Ideal, das man als „verteilte“ (oder vollständig dezentralisierte) Bestätigung bezeichnen könnte. Der schwächste wäre ein Miner mit 100 % der Hash-Power, was einer „zentralisierten“ Bestätigung entspräche.

Genauer gesagt, das im Bezug auf die Bestätigung dezentralisierteste System ist das mit der größten Anzahl an Vertizes (Minern) mit der höchsten Gewichtsverteilung (Hash-Power):

```
Bestätigungsdezentralisierung = Verteilung(Hash-Power) * Miner
```

Referenzen

[1] https://de.wikipedia.org/wiki/Variationskoeffizient

[2] https://en.wikipedia.org/wiki/Null_graph

Sicherheitsmodell

Dezentralisierung allein bedeutet keine Sicherheit. Sicherheit ist das Produkt von Aktivität, der Verteilung dieser Aktivität und dem Anteil der beteiligten Menschheit.

```
Sicherheit = Aktivität * Verteilung * Beteiligung
```

Da es keine Grenzen für die Menschheit, den Handel oder Rechenleistung gibt, ist das Sicherheitsniveau in jeder Achse unbegrenzt. Sicherheit ist auch bei perfekter Verteilung (d. h. unendlicher Dezentralisierung) unbegrenzt. Ein Mindestniveau von null wird in jeder Achse erreicht, wenn entweder keine Teilnahme oder keine Aktivität stattfindet. Wirtschaftliche und Bestätigungssicherheit können daher wie folgt definiert werden:

```
Wirtschaftliche Sicherheit = Einnahmen * Verteilung(Einnahmen) * [Händler /
Menschheit]

Bestätigungssicherheit = Hash-Power * Verteilung(Hash-Power) * [Miner /
Menschheit]
```

Grenzen des Modells

Diese Beziehungen sagen nichts über die absolute Wirksamkeit aus, die ein Wert repräsentiert, oder über die relative Wirksamkeit zweier beliebiger Werte, außer dass ein höherer Wert eine höhere Wirksamkeit repräsentiert. Dies liegt nicht an einem Mangel des Modells. Zu den Faktoren gehören Menschen, insbesondere die Wirksamkeit ihrer individuellen Widerstandsfähigkeit[1] und ihre Wahrnehmung des Werts des Geldes. Alle, die validieren oder minen, bieten ein gewisses Maß an Widerstand, aber es gibt keine implizite Kontinuität. Wir sprechen von einem „Niveau“ an Sicherheit, nicht von einem „Umfang“ an Sicherheit.

Referenzen

[1] Kapitel: Widerstandsaxiom

Wie im Prinzip der öffentlichen Daten[1] gezeigt, ist Anonymität ein Werkzeug, das dabei hilft, die eigene Fähigkeit zum Handeln und/oder Mining zu schützen. Der Grad der Dezentralisierung kann als solches nie gemessen werden; das Modell ist eine konzeptionelle Hilfe. Wie der Fehlschluss des Kräftegleichgewichts[2] zeigt, ist die von den beiden Untermodellen gebotene Sicherheit komplementär und unabhängig voneinander. Während die Menschen in Zukunft beschließen könnten, unabhängig zu handeln und/oder zu minen, zeigt der Kakerlakenfehlschluss[3] , dass sie erst dann zur Sicherheit beitragen, wenn sie dies auch tun. Das Modell stellt die Sicherheit dar, wie sie in diesem Zeitraum existiert.

Referenzen

[1] Kapitel: Prinzip der öffentlichen Daten

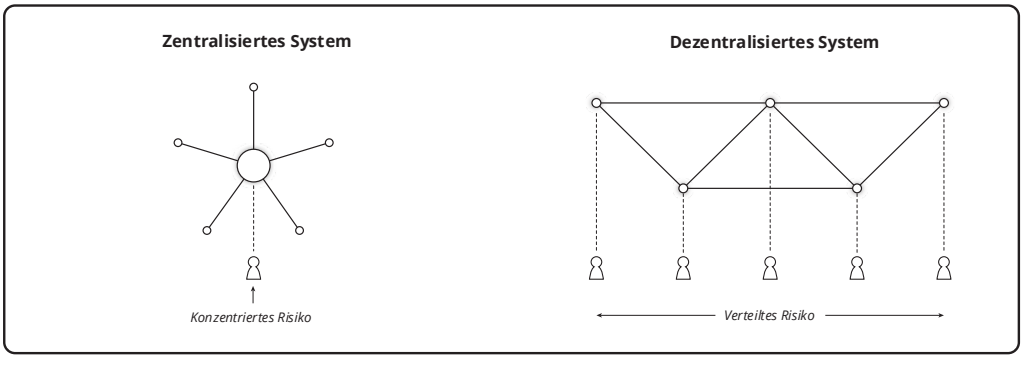
[2] Kapitel: Fehlschluss des Kräftegleichgewichts

[3] Kapitel: Kakerlakenfehlschluss

Risikoverteilungsprinzip

Bitcoin wird nicht durch Blockchains[1], Hash Power, Validierung, Dezentralisierung, Kryptographie[2], Open Source[3] oder Spieltheorie[4] abgesichert – es wird von Menschen abgesichert.

Technologie ist niemals die Wurzel der Systemsicherheit. Technologie ist ein Werkzeug, das Menschen hilft, das zu sichern, was sie wertschätzen. Sicherheit erfordert, dass Menschen handeln. Ein Server kann nicht durch eine Firewall gesichert werden, wenn an der Tür zum Serverraum kein Schloss vorhanden ist, und ein Schloss kann den Serverraum nicht sichern, ohne dass ein Wachmann die Tür überwacht, und ein Wachmann kann die Tür nicht sichern, ohne dass er seine Haut riskiert.



Bei Bitcoin ist das nicht anders, es wird von Menschen gesichert, die sich einem persönlichen Risiko aussetzen. Dieses Risiko mit anderen Menschen zu teilen, ist der

Referenzen

[1] https://de.wikipedia.org/wiki/Blockchain

[2] https://de.wikipedia.org/wiki/Kryptographie

[3] https://de.wikipedia.org/wiki/Free/Libre_Open_Source_Software

[4] Kapitel: Fehlschluss des Gefangenendilemmas

Zweck der Dezentralisierung. Ein zentralisiertes System[1] erfordert eine Person[2], um das gesamte Risiko zu tragen. Ein dezentralisiertes System teilt das Risiko unter Einzelpersonen[3] auf, die die Systemsicherheit umfassen. Wer den Wert der Dezentralisierung nicht versteht, der versteht die notwendige Rolle[4] der Menschen für die Sicherheit höchstwahrscheinlich auch nicht.

Bitcoin ermöglicht es den Menschen, das persönliche Risiko der Annahme und des Minings von Coins zu teilen. Es sind ihre Bereitschaft und Fähigkeit zum Widerstand[5], die die Nötigung ihrer Nodes und Übernahme ihrer Minen verhindern, und das ist es, was Bitcoin tatsächlich sichert. Wenn Menschen diese Risiken nicht akzeptieren, gibt es keine wirksame Sicherheit im Geld. Wenn sehr viele Menschen dies tun, wird das individuelle Risiko minimiert. Bitcoin ist ein Werkzeug, keine Magie.

Referenzen

[1] https://de.wikipedia.org/wiki/Liberty_Reserve

[2] https://de.wikipedia.org/wiki/Ross_Ulbricht

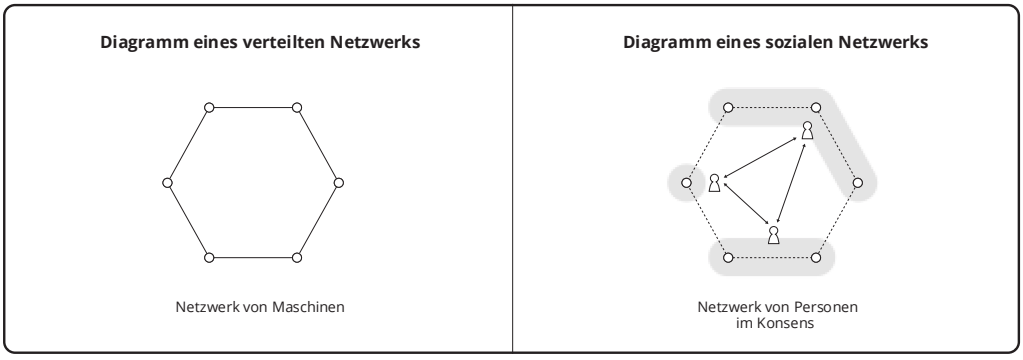
[3] https://de.wikipedia.org/wiki/BitTorrent

[4] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177

[5] Kapitel: Widerstandsaxiom

Prinzip des sozialen Netzwerks

In der Terminologie von Paul Barans Aufsatz über verteilte Netzwerke aus dem Jahr 1964[1] liegt die Bedeutung der Topologie beim Netzwerk in der Fähigkeit der Kommunikation, dem Verlust einer bestimmten Anzahl von Knoten standzuhalten. Ein zentralisiertes (Stern-)Netzwerk wird beim Verlust eines Knotens scheitern. Ein verteiltes (Mesh-)Netzwerk ist widerstandsfähiger. Ein Hybrid dieser Systeme wird als dezentral betrachtet.



Als Geld bildet Bitcoin einen sozialen Graphen. Nur eine Einzelperson kann sich entscheiden, das eine oder andere Geld[2] im Tausch anzunehmen. Eine Gruppe von Personen, die die gleiche Definition von Geld teilen, wird als Konsens bezeichnet. Autorität in einem Währungssystem ist die Macht, das Geld zu definieren. Bitcoin ist ein Werkzeug, mit dem sich Menschen gegen die Tendenz zur Autorität wehren können, um ihre Zustimmung zum und damit den Nutzen des Geldes zu wahren.

In der Terminologie verteilter Systeme ist ein Bitcoin-"Knoten" eine Person und das System ist Geld. Es spielt keine Rolle, wie viele Maschinen diese Person steuert, der

Referenzen

[1] http://web.cs.ucla.edu/classes/cs217/Baran64.pdf

[2] Kapitel: Taxonomie des Geldes

Verlust dieser Person bedeutet den Verlust eines Knotens im Netzwerk (einschließlich aller Maschinen dieser Person).

Ein zentralisiertes Geld kann den Verlust einer Person nicht verkraften. Wenn diese eine Person ihre Regeln ändert, hört das ursprüngliche Geld auf zu existieren. Wie im Risikoverteilungsprinzip[1] gezeigt, verlässt sich Bitcoin auf Dezentralisierung, um es den Menschen zu ermöglichen, sich einer Autorität zu widersetzen[2]. Durch diese Dezentralisierung ist das Geld widerstandsfähiger gegen den Verlust weiterer Menschen durch staatliche Angriffe. Ein Verlust in diesem Sinne ist die Weigerung der Person, mit dem Geld zu handeln.

Referenzen

[1] Kapitel: Risikoverteilungsprinzip

[2] Kapitel: Widerstandsaxiom

Gefährdungsstufenparadoxon

Wie die Nullsummeneigenschaft[1] impliziert, besteht die einzige Möglichkeit externe Subventionen[2] zu überwinden, darin, mit einem Kapitalverlust im Verhältnis zur marktüblichen Kapitalrendite zu minen. Gleichermaßen scheint es so, als ob die einzige Möglichkeit, Besteuerung bis hin zu 100 % (Verbot) zu vermeiden, darin besteht, dass außerhalb der Reichweite der Steuerbehörde, also im Geheimen, gemined wird. Wie bei allen Schwarzmärkten[3] ist das subversive Mining[4] mit höheren Kosten verbunden. Der Wettbewerb mit subventioniertem Mining erhöht die Kosten.

Wenn man das Widerstandsaxiom[5] akzeptiert, muss man davon ausgehen, dass sowohl Steuern als auch Subventionen verwendet werden, um die Kosten für die Kontrolle von Bitcoin zu senken. Durch die Möglichkeit, das Mining (über Steuereinnahmen) zu subventionieren, können Staaten eine Kartellierung im Subventionsbereich bewirken. Sobald die mehrheitliche Hash Power konzentriert ist, kann der Staat seine Steuer-(Regulierungs-)Macht in der Region nutzen, um Zensur zu erzwingen.

Um also in den Genuss eines Bitcoins zu kommen, scheint es, dass Personen letztendlich mit Verlust minen müssen. Zensur schafft jedoch die Möglichkeit für andere, gewinnbringend zu minen, sofern die Menschen bereit sind, diese Kosten durch Gebühren auszugleichen. Dieser Schwarzmarkt ist Bitcoins Zensurresistenz.

Referenzen

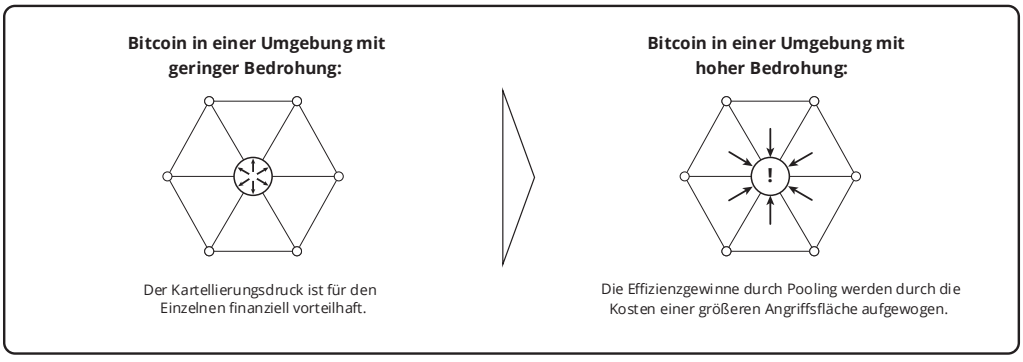
[1] Kapitel: Nullsummeneigenschaft

[2] https://de.wikipedia.org/wiki/Subvention

[3] https://de.wikipedia.org/wiki/Schwarzmarkt

[4] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177

[5] Kapitel: Widerstandsaxiom



Die Menschen zahlen für bestimmte Transaktionen einen höheren Preis, und um diesen höheren Preis aufrechtzuerhalten, muss der Staat die Kosten genauso tragen, obwohl diese ineffektiv sind.

Paradoxerweise funktioniert dieses Werkzeug gut, wenn das Geld angegriffen wird und schlecht andernfalls. Gäbe es keinen *internen* Kartellierungsdruck[1] wären diese Fälle ausgeglichen. Aber Risikoverteilung[2] ist für das subversive Mining essenziell, und Kartellierungsdruck wirkt der Verteilung *entgegen*. Die Angriffsfläche[3] vergrößert sich also ständig ohne Druck zur Kontraktion, es sei denn, effektive monetäre Alternativen werden unterdrückt. Die Unterdrückung[4] von Alternativen erhöht den Nutzen der Belohnung für den Miner im Bereich der Unterdrückung. Dieses Paradox gilt ebenso für den Zentralisierungsdruck[5].

Die zu erwartende Konsequenz ist, dass Bitcoin nicht gut auf Angriffe vorbereitet sein wird, da dies für Menschen in einem Umfeld mit geringer Bedrohungslage finanziell nachteilig ist.

Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

[2] Kapitel: Risikoverteilungsprinzip

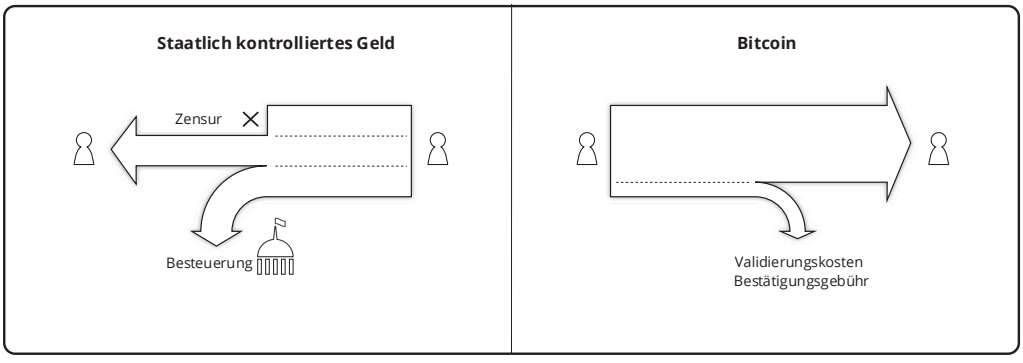
[3] https://en.wikipedia.org/wiki/Attack_surface

[4] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

[5] Kapitel: Zentralisierungsrisiko

Wertversprechen

Der Wert von Bitcoin gegenüber seinen Alternativen ergibt sich direkt aus der Entfernung der Kontrolle des Staates sowohl über die Geldmenge als auch die Zensur von Transaktionen. Zu den Vorteilen zählen Freiheit von Seigniorage[1], Devisenverkehrsbeschränkung[2], und Finanzüberwachung[3]. Diese ermöglichen die Überweisung des Geldes an jede Person, an jedem Ort, zu jeder Zeit, ohne dass die Erlaubnis eines Dritten erforderlich wäre.



Diese Vorteile stellen eine Kostensenkung durch Steuervermeidung dar. Seigniorage ist eine direkte Steuer, während Devisenkontrollen deren Umgehung einschränken. Der Staat selbst behauptet häufig politische Unabhängigkeit[4] als Ziel, um diese Steuermacht einzuschränken. Finanzüberwachung begrenzt Steuerhinterziehung im Allgemeinen. **Auch wenn Bitcoin die Steuern nicht beseitigen oder die Gesamtabgaben nicht zwangsläufig reduzieren kann, stellt es doch eine Änderung in der Art der Besteuerung**

Referenzen

[1] https://de.wikipedia.org/wiki/Seigniorage

[2] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

[3] https://de.wikipedia.org/wiki/Know_your_customer

[4] https://www.federalreserve.gov/faqs/about_12799.htm

dar. Für diejenigen, die den Staat als soziales Gut betrachten, bleibt auf jeden Fall die Option, ihn freiwillig zu finanzieren.

Es wäre ein Fehler anzunehmen, dass diese Vorteile aus der Existenz einer effizienteren Technologie resultieren als die, die von Monopolgeldern[1] eingesetzt wird. Die Technologie ist weitaus weniger effizient[2], dennoch hilft sie den Menschen[3], sich staatlichen Kontrollen zu widersetzen. Es ist dieser Widerstand[4], der den Wert liefert.

Referenzen

[1] Kapitel: Taxonomie des Geldes

[2] Kapitel: Skalierungsprinzip

[3] Kapitel: Risikoverteilungsprinzip

[4] Kapitel: Widerstandsaxiom

ETATIMUS

Ziele eines Fedcoin

Wie in Wertversprechen[1] beschrieben, gibt es zwei Aspekte an Bitcoin, die ihn zu einem Ziel staatlicher Kontrollen machen, denn beide stellen eine Bedrohung der Steuereinnahmen dar.

Im Kampf[2] gegen Bitcoin könnte der Staat versuchen, ein äußerlich ähnliches Geld[3] einzuführen, welches als Fedcoin bezeichnet werden könnte. Dieses könnte als Abspaltung oder alternativer Coin eingeführt werden. Das Ziel wäre es, die oberflächlichen Aspekte von Bitcoin zu bewahren und gleichzeitig sein Wertversprechen zu eliminieren. Dies würde Steuereinnahmen schützen und gleichzeitig den Befürwortern ermöglichen, Fedcoin als „sicherere" Alternative zu Bitcoin zu propagieren. Fedcoin selbst ist für Bitcoin nicht relevant, außer insoweit, als der Akt, seine Verwendung zu erzwingen, Widerstand[4] erfordert.

Die wesentlichen Unterschiede zwischen Fedcoin und Bitcoin ermöglichen es dem Staat, willkürlich neue Einheiten zu erzeugen (Seigniorage[5]) und deren Transfer zu verweigern (Zensur). Das Ziel der Seigniorage kann durch einen Hard-Fork erreicht werden, der eine neue Konsenregel einführt. Diese Regel erlaubt die Einführung neuer Einheiten, wenn der Staat eine inflationäre Transaktion signiert hat. Das Zensurziel kann durch einen Soft-Fork erreicht werden, der die Bestätigung von Transaktionen ohne staatliche Signatur verhindert.

Referenzen

[1] Kapitel: Wertversprechen

[2] Kapitel: Prinzip der anderen Mittel

[3] Kapitel: Taxonomie des Geldes

[4] Kapitel: Widerstandsaxiom

[5] https://de.wikipedia.org/wiki/Seigniorage

Den Staat daran zu hindern, die Verwendung dieser Forks zu erzwingen, ist der zentrale Zweck der Systemsicherheit von Bitcoin. Die Wirtschaft schützt vor dem Hard-Fork, die Miner schützen vor dem Soft-Fork. Die von diesen Menschen eingegangenen Risiken[1] bewahren den Wert des Geldes im Vergleich zu staatlich kontrollierten Alternativen.

Referenzen

[1] Kapitel: Risikoverteilungsprinzip

Fehlschluss der inflationären Qualität

Es gibt eine Theorie, dass die durch Seigniorage[1] verursachte Preisinflation[2] zur Produktion von Gütern geringerer "Qualität" und/oder geringerer Haltbarkeit[3] führt. Haltbarkeit ist eine von vielen Eigenschaften, die eine Person einer anderen an einem Gut vorziehen kann. **Die Theorie geht zwangsläufig davon aus, dass der Wert objektiv ist und widerspricht daher der Theorie des subjektiven Werts.** Daher ist die Theorie ungültig.

Es besteht kein nachweisbarer Zusammenhang zwischen der Anzahl der Einheiten des Geldes[4], die zum Tausch gegen ein Gut erforderlich sind, und den Qualitäten eines Gutes, die man bevorzugen könnte. Größerer Wohlstand (der eine Auffassung ist, da Wert subjektiv[5] ist) bedingt eine geringere Zeitpräferenz[6], wie in Theorie des Grenznutzens[7] gezeigt wird. Doch selbst wenn man von einer Fehleinschätzung des zunehmenden Wohlstands ausgeht, bedeutet eine geringere Zeitpräferenz nicht automatisch eine Präferenz für Güter von geringerer Qualität. Sie impliziert lediglich eine zunehmende Bereitschaft, einen größeren Teil des eigenen Kapitals zu verleihen. Rothbard[8] begeht in seinem Buch *Was hat die Regierung mit unserem Geld gemacht?*[9] den „subtilen" Fehler, der auch heute noch fortbesteht.

Referenzen

[1] https://de.wikipedia.org/wiki/Seigniorage

[2] https://de.wikipedia.org/wiki/Inflation

[3] Kapitel: Abschreibungsprinzip

[4] Kapitel: Taxonomie des Geldes

[5] https://en.wikipedia.org/wiki/Subjective_theory_of_value

[6] Kapitel: Zeitpräferenzfehlschluss

[7] https://de.wikipedia.org/wiki/Grenznutzen

[8] https://de.wikipedia.org/wiki/Murray_Rothbard

[9] https://mises.org/online-book/what-has-government-done-our-money/iii-government-meddling-money/2-economic-effects-inflation

> Die Qualität der Arbeit nimmt während einer Inflation aus einem subtileren Grund ab: Die Menschen verlieben sich in „Schnell-reich-werden-Programme“, die in einer Zeit ständig steigender Preise scheinbar in Reichweite ihrer Möglichkeiten liegen, und verachten oft ernsthafte Anstrengungen.
>
> *Murray Rothbard: Was hat die Regierung mit unserem Geld gemacht?*

Es wird angenommen, zumindest von Rothbard, dass die Menschen es *immer* vorziehen, früher als später reich zu werden, wie es das Axiom der Zeitpräferenz impliziert. Und wie der Fisher-Effekt[1] zeigt, wird die Preisinflation, sofern sie vorhersehbar ist, durch den Realzins[2] ausgeglichen. Sofern sie nicht vorhersehbar ist, gilt Rothbards Vermutung nicht.

Seigniorage ist eine Steuer, die Menschen ärmer macht. Ärmer zu sein *erhöht* die Zeitpräferenz, das Gegenteil des von der Theorie beschriebenen Effekts. Jede Steuer verschiebt unfreiwillig Eigentum von einigen Leuten auf andere, denn das ist ihr einziger tatsächlicher Mechanismus bzw. ihr einziges Ziel. Wie Rothbard selbst in seinem wesentlich strengeren Werk *Mensch, Wirtschaft und Staat*[3] ausführt, ist die Form der Steuer ökonomisch irrelevant.

> Aus all diesen Gründen ist das Ziel einer einheitlichen Besteuerung ein unmögliches. Es ist nicht nur in der Praxis schwer zu erreichen; es ist auch konzeptionell unmöglich und widersprüchlich.
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Daher kann nicht einmal nachgewiesen werden, dass die Seigniorage selbst die Besteuerten ärmer macht als die Steuern, die sie angeblich ersetzt. Nur eine Nettosteuererhöhung bedeutet eine Vermögensminderung.

Referenzen

[1] https://de.wikipedia.org/wiki/Fisher-Effekt

[2] https://de.wikipedia.org/wiki/Realzins

[3] https://mises.org/library/man-economy-and-state-power-and-market/html/ppp/1393

Reserveprinzip

Der Begriff „Reserve"[1] bezieht sich auf einen Kapitalvorrat (Hort), im Unterschied zu dem Teil der Ersparnisse, der investiert ist. Sowohl Staaten als auch Menschen horten Kapital, um den erwarteten Liquiditätsbedarf zu decken. Der Begriff „Reservewährung"[2] bezieht sich auf einen staatlichen Hort, der zur Abrechnung[3] von Konten mit anderen Staaten erforderlich ist. Die Geldreserven der Bürger eines Staates bestehen im Allgemeinen aus dem vom Staat ausgegebenen Geld – hauptsächlich Banknoten oder Fiatgeld, zu einem geringeren Anteil in Münzen[4].

Staaten kaufen Reservewährungen von den Menschen, indem sie Monopolgeld[5], Devisenkontrollen[6] und direkte Besteuerung verwenden. Durch die Verwendung des eigenen Geldes werden Käufe um den Betrag der Seigniorage[7] abgezinst. Devisenkontrollen beschränken oder verbieten die Verwendung der Reservewährung als Geld. Indem der Staat die Reservewährung als Eigentum und nicht als Geld behandelt, erhebt er eine Steuer auf den scheinbaren Kapitalgewinn[8] des Reservegeldes, wenn er sein Geld durch Geldinflation[9] gegen die Reservewährung abwertet[10]. Offizielle

Referenzen

[1] Kapitel: Definition der Reserve

[2] https://de.wikipedia.org/wiki/Leitwährung

[3] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)

[4] https://de.wikipedia.org/wiki/Primitivgeld

[5] Kapitel: Taxonomie des Geldes

[6] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

[7] https://de.wikipedia.org/wiki/Seigniorage

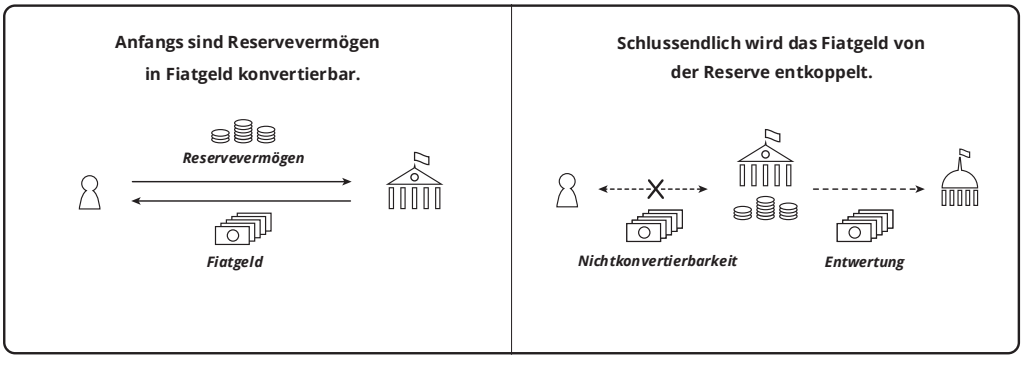
[8] https://www.investopedia.com/articles/personal-finance/081616/understanding-taxes-physical-goldsilver-investments.asp

[9] https://en.wikipedia.org/wiki/Monetary_inflation

[10] https://de.wikipedia.org/wiki/Inflation

Wechselkurse[1] unterhalb des Marktwerts führen zu einer weiteren Steuer auf die Verwendung der Reservewährung.

Ein „Goldstandard“ ist ein Standard, bei dem der Staat Gold als Devisenreserve einnimmt und Privatpersonen es in Form von Forderungen gegen einen „Standard-Betrag“ zurücklegen. Der US-Dollar wurde 1834 eingeführt[2], einlösbar in Gold zu 20,67 USD pro Unze. 100 Jahre lang kaufte und verkaufte der Staat Gold zu diesem Kurs. 1934 wurde der Dollar um 60 % auf 35 USD pro Unze abgewertet[3]. Zu diesem Zeitpunkt wurde seine Einlösbarkeit (durch die Bevölkerung) aufgehoben und es wurde für sie ungesetzlich, ihn zu horten oder Verträge in ihm abzuschließen. Diese Uneinlösbarkeitsregelung wurde 1971 auf andere Staaten ausgeweitet[4], was den Goldstandard in den Vereinigten Staaten offiziell beendete. Da der Dollar keine Staatsschuld mehr war, wurde er von einer repräsentativen Währung[5] (d.h. Banknote) zu einer Fiatwährung.



Referenzen

[1] https://de.wikipedia.org/wiki/Wechselkurs

[2] https://en.wikipedia.org/wiki/Coinage_Act_of_1834

[3] https://en.wikipedia.org/wiki/Gold_Reserve_Act

[4] https://de.wikipedia.org/wiki/Nixon-Schock

[5] https://en.wikipedia.org/wiki/Representative_money

Die wichtigste Devisenreserve der USA ist Gold[1] (74,5 %), der Rest sind ausländische Währungen und Äquivalente, während die Bürger hauptsächlich in Dollar reservieren. Die eigenen Banknoten oder Fiatgeld eines Staates sind im Allgemeinen nicht als eigene Devisenreserve nutzbar, da der Staat seine Zahlung annullieren oder abwerten kann.

Das US-Finanzministerium berichtet, dass es über 8.000 Tonnen Gold im Wert von etwa 400.000.000.000 US-Dollar hortet[2]. Die Kaufkraft der US-Dollarnote im Jahr 1834 war etwa 30-mal so hoch wie die des US-Dollars im Jahr 2019.

Der Zweck einer Reservewährung ist die Besteuerung. Der Staat kauft zunächst das Reservegeld mit handelbaren Wertpapieren[3], gibt dann mehr Scheine aus, als er in Reserve hat, erklärt die Scheine für ungültig und behält die Reserve ein. Die Entwertung der Banknoten ist das Ergebnis einer übermäßigen Ausgabe (Seigniorage) und stellt eine Steuer für diejenigen dar, die sie horten. Der Staat sammelt das Reservegeld in seinem Hort, der seine Fähigkeit darstellt, seine eigenen Schulden bei anderen Staaten zu begleichen. Zwar horten die Menschen das Reservegeld noch immer, doch unterliegt seine Verwendung strengen Beschränkungen[4], um die Steuervorteile des staatlichen Monopolgeldes zu erhalten. Diese Beschränkungen verschärfen sich, wenn die Höhe der Steuern steigt.

Die Verwendung von Gold als staatliche Reserve bietet keinen monetären Vorteil für Einzelpersonen, die weiterhin mit Monopolgeld handeln müssen. Wie in Fehlschluss der Reservewährung[5] gezeigt, kann Bitcoin als staatliche Reserve nicht besser abschneiden. Anders als bei Gold liegt die Definition von Bitcoin jedoch in den Händen derjenigen, die

Referenzen

[1] https://de.wikipedia.org/wiki/Goldreserve

[2] https://www.treasury.gov/resource-center/data-chart-center/IR-Position/Pages/01042019.aspx

[3] https://de.wikipedia.org/wiki/Wechsel_(Wertpapier)

[4] https://www.reuters.com/article/us-venezuela-economy/venezuela-loosens-currency-exchange-controls-to-allow-forex-trading-idUSKCN1SD2NC

[5] Kapitel: Fehlschluss der Reservewährung

es im Handel akzeptieren. Läge der Großteil der tatsächlichen Akzeptanz von Bitcoin in den Händen des Staates und handelten die Menschen mit Geldsubstituten[1], könnte nichts den Staat daran hindern, sowohl willkürliche Inflation als auch Zensur einzuführen.

Referenzen

[1] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

Fehlschluss der Reservewährung

Es gibt eine Theorie, dass Bitcoin schlussendlich von Staaten als Reservewährung[1] gehalten wird und dass Einzelpersonen Transaktionen mit durch Bitcoin „gedecktem" Monopolgeld[2] durchführen. Die Theorie besagt, dass das Transaktionsvolumen für die Verwendung als Verbraucherwährung nicht ausreicht, die Fähigkeit, Geldinflation[3] zu verhindern, Bitcoin aber zur idealen Reservewährung macht. Zentralbanken und deren autorisierte Funktionäre würden handelbare Wechsel[4] ausgeben und gleichzeitig Bitcoin in Reserve halten. Da Bitcoin nicht inflationiert werden kann, wären die zahlreichen Probleme, die durch die staatliche Kontrolle des Geldes entstehen, gelöst und eine neue Ära des Wohlstands eingeläutet. Die Transaktionsgebühren wären niedrig, während das Transaktionsvolumen unbegrenzt wäre.

Betrachten wir das Szenario, während es sich entfaltet. Bitcoin entwickelt sich zu einer weit verbreiteten Währung[5], hat aber mit geringem Transaktionsvolumen, hohen Gebühren und langen Bestätigungszeiten zu kämpfen. Um eine Reserve in Bitcoin (BTC) zu erhalten, gibt der Staat im Tausch gegen Bitcoin handelbare[6] Bitcoin-Zertifikate (BZ) aus. Dies kann durch die Beschlagnahmung zentralisierter Konten (zwingende Konvertierung) oder durch Markthandel erreicht werden, wobei beide Maßnahmen schon einmal zum Aufbau von Goldreserven durchgeführt wurden. Es wird ein Prüfungsprozess eingerichtet, mit dem Personen überprüfen können, dass die ausgegebenen BZ niemals die BTC-Reserven überschreiten. Es werden Zahlungsmittelgesetze[7] geschaffen, die von den Menschen verlangen, BZ als

Referenzen

[1] Kapitel: Reserveprinzip

[2] Kapitel: Taxonomie des Geldes

[3] https://en.wikipedia.org/wiki/Monetary_inflation

[4] https://de.wikipedia.org/wiki/Wechsel_(Wertpapier)

[5] https://de.wikipedia.org/wiki/Währung

[6] https://en.wikipedia.org/wiki/Negotiable_instrument

[7] https://de.wikipedia.org/wiki/Zahlungsmittel

Zahlungsmittel für die Begleichung von Schulden zu akzeptieren, sofern nicht ausdrücklich etwas anderes vereinbart wurde. Die Leute kaufen BZ mit BTC, damit sie Steuern zahlen und Dinge bei Einzelhändlern auf dem Weißmarkt kaufen können. Letztendlich werden die meisten BTC als staatliche Reserven gehalten.

Dieses Szenario dürfte Ihnen bekannt vorkommen, denn auf diese Weise gelangten Staaten zu Gold und Menschen wurden mit Papier abgespeist. Die Theorie ist auf mehreren Ebenen ungültig.

Das Verhältnis von ausgegebenem BZ zu BTC in Reserve kann niemals effektiv überprüft werden. Selbst wenn die Bitcoin-Konsensregeln irgendwie bestehen bleiben, gibt es *keine Möglichkeit* zu wissen, wie viel BZ ausgegeben wurde, und es gibt keinen Regress, wenn eine Entwertung vermutet wird. Man muss der Zentralbank *vertrauen*, dass sie für die BZ-Emission Rechenschaft ablegt und letztlich bedeutet das, dass jeder darauf vertraut, dass der Staat keine Lockerungsmaßnahmen[1] durchführt. Die Geschichte zeigt, dass dies unwahrscheinlich ist, und außerdem stellt es keine Verbesserung gegenüber den derzeitigen Staatsgeldern dar.

Warum kann eine Person BZ also niemals effektiv überprüfen, wie es mit BTC, welches es ersetzt hat, möglich ist? Weil BZ dadurch nicht von den in Reserve gehaltenen BTC unterscheidbar wären. Mit anderen Worten, der *Grund*, dass es überhaupt einen Unterschied zwischen Zahlungsmittel und Reservewährung gibt, ist der, die Inflation der verwendeten Währung zu ermöglichen (Besteuerung[2]) und gleichzeitig ein besseres Geld[3] in Reserve zu halten (horten).

Darüber hinaus muss es für die Existenz von Bitcoin eine tatsächliche dezentrale Bitcoin-Wirtschaft geben. Ohne Einzelpersonen, die im Handel erhaltene BTC validieren, gibt es

Referenzen

[1] https://de.wikipedia.org/wiki/Quantitative_Lockerung

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] https://de.wikipedia.org/wiki/Greshamsches_Gesetz

niemanden, der ungültige BTC ablehnen könnte, da diese durch den Staat neu definiert werden[1]. In diesem Fall können leicht Zensur[2] und Inflation eingeführt werden, was die Theorie entkräftet. Nur Schwarzmarkt-Bitcoin-Transaktionen und -Mining können diesem Übergang widerstehen[3]. Dadurch entsteht kaum wirtschaftlicher Druck auf den Staat, die Konsensregeln von Bitcoin einzuhalten.

Durch Schichtung bleiben die Kryptodynamischen Prinzipien[4] der Dezentralisierung erhalten, während "Deckung" die völlige Abkehr davon bedeutet. Bitcoin kann nicht überwiegend als Deckungsgeld für Zentralbanknoten aufrechterhalten werden. Damit es sicher ist, müssen Menschen damit handeln.

Es ist durchaus möglich, dass Bitcoin von Staatskassen gehalten wird, aber dies bietet den Menschen keine Transaktionsskalierung oder andere Vorteile.

Referenzen

[1] Kapitel: Ziele eines Fedcoin

[2] Kapitel: Eigenschaft der Zensurresistenz

[3] Kapitel: Widerstandsaxiom

[4] Kapitel: Kryptodynamische Prinzipien

Staatsbankenprinzip

Im freien Bankwesen[1] gibt es keinen tatsächlichen Kreditgeber der letzten Instanz[2], es impliziert lediglich einen weiteren Kreditgeber, der den im Aus-dem-Nichts-Fehlschluss[3] aufgezeigten Einschränkungen unterliegt. Im staatlichen Bankwesen ist dies jedoch die Zentralbank[4], unterstützt vom Steuerzahler. Der Staat erhebt Steuern, um den Mitgliedsbanken[5] und der Staatskasse zinsgünstige Kredite[6] zu gewähren. Die Kredite müssen mit einem Abschlag auf die marktüblichen Zinsen[7] versehen sein, da es sich sonst nicht um einen letzten Ausweg handelt. Banken haben jederzeit die Möglichkeit, Kredite bei anderen Banken und potenziellen Einlegern aufzunehmen. Zur Unterstützung dieses Abschlags ist eine Besteuerung erforderlich. Wenn der wirtschaftliche Zinssatz also 10 % beträgt, kann der Staat den Mitgliedsbanken Kredite zu 3 % gewähren und die Differenz durch Steuern decken.

Der Staat verfügt über viele Steuereinnahmequellen, aber in der Regel subventionieren Zentralbanken ermäßigte Kreditzinsen mit Seigniorage[8]. Zentralbanken sind dafür bekannt, zu verkünden, dass sie kein „Geld drucken“, aber genau das tun sie. Die U.S. Federal Reserve[9] (“Fed”) hat die Macht, neues Geld[10] beim US-Finanzministerium[11]

Referenzen

[1] https://en.wikipedia.org/wiki/Free_banking

[2] https://de.wikipedia.org/wiki/Kreditgeber_letzter_Instanz

[3] Kapitel: Aus-dem-Nichts-Fehlschluss

[4] https://de.wikipedia.org/wiki/Zentralbank

[5] https://en.wikipedia.org/wiki/Structure_of_the_Federal_Reserve_System

[6] https://de.wikipedia.org/wiki/Spitzenrefinanzierungsfazilität

[7] https://www.frbdiscountwindow.org/pages/discount-rates/current-discount-rates

[8] https://de.wikipedia.org/wiki/Seigniorage

[9] https://en.wikipedia.org/wiki/Federal_Reserve

[10] https://www.frbservices.org/financial-services/cash/

[11] https://www.bep.gov/

anzufordern. Die Fed zahlt die Druckkosten[1] für "Papiergeld" (eigentlich Stoff[2]) und den Nennwert für die Münze[3]. Das Finanzministerium ist lediglich der Auftragnehmer, der die Arbeiten ausführt. Typischerweise werden Münzen so hergestellt, dass sie einen etwas höheren Nennwert als den Gebrauchswert[4] haben, um das Verschwinden[5] der Münzen zu verhindern. Dieser Gebrauchswert muss daher reduziert werden, wenn der Nennwert im Verhältnis dazu infolge der Abwertung des entsprechenden Fiatgeldes sinkt.

Dies impliziert, dass die monetäre Inflation[6] des staatlichen Fiatgeldes buchstäblich die Folge des Druckens des „Papiergeldes" ist. Dieser Prozess ist etwas undurchsichtig. Die Fed druckt das Geld nicht erst, stopft es in einen Tresor und verleiht es dann. Das ist unnötig. In der Praxis ist die Reihenfolge umgekehrt. Die Fed vergibt diskontierte Kredite, in der *Annahme*, dass sich Geld in ihrem Tresor befindet.

Der von der Fed eingeführte Abwicklungsprozess[7] überwacht, wie viel Geld sich in den Reserven jeder Mitgliedsbank befindet. Der Großteil der Abwicklungen kann oft saldiert[8] werden, aber in regelmäßigen Abständen muss das Geld physisch bewegt werden.

Um die Transportkosten weiter zu senken, muss ein erheblicher Teil der Reserven der Mitgliedsbanken in den eigenen Tresoren der Fed verwahrt werden. Dies kann durch den Kauf von Staatsanleihen (Treasuries[9]) erreicht werden, die von der Fed zum Verkauf

Referenzen

[1] https://www.federalreserve.gov/faqs/currency_12771.htm
[2] https://www.bep.gov/currency/how-money-is-made
[3] https://de.wikipedia.org/wiki/Münze
[4] https://de.wikipedia.org/wiki/Gebrauchswert
[5] https://de.wikipedia.org/wiki/Greshamsches_Gesetz
[6] https://en.wikipedia.org/wiki/Monetary_inflation
[7] https://de.wikipedia.org/wiki/Fedwire
[8] https://en.wikipedia.org/wiki/Set-off_(law)#Close_out_netting
[9] https://en.wikipedia.org/wiki/United_States_Treasury_security

angeboten werden[1]. Dabei handelt es sich um Geldersatz[2], der als ausreichend angesehen wird, um die Mindestreserveanforderungen der Mitgliedsbanken zu erfüllen. Staatsanleihen sind Schuldtitel, die vom US-Finanzministerium ausgegeben und in der Regel in großen Mengen auf dem freien Markt[3] von der Fed gekauft werden. Die Fed reduziert die Rendite von Staatsanleihen (d. h. den vom Staat gezahlten Zinssatz), indem sie für eine erhöhte Nachfrage sorgt. Sie finanziert diese Geschäfte im Wesentlichen auf die gleiche Weise wie diskontierte Kredite an ihre Mitgliedsbanken. Der Unterschied besteht lediglich darin, dass es sich bei diesen Käufen um diskontierte Kredite an den Staat handelt.

Die Fed kann *vorgeben* sie hätte Geld in ihrem Tresor und es nur so drucken, wie es für die Abwicklung benötigt wird. Dadurch entsteht die Illusion, die Geldinflation sei das Ergebnis der Kreditvergabe. Tatsächlich ist sie jedoch ausschließlich das Ergebnis der Fähigkeit der Fed, Geld mit einem Abschlag zu kaufen und so die Kredite zu finanzieren. Wenn eine Mitgliedsbank Geld benötigt, kann sie es von der Fed mit Staatsanleihen kaufen. Wenn die Reserven der Fed an tatsächlichem Geld nicht ausreichen, nimmt sie einfach eine „Abhebung" vom Steuerzahler vor, indem sie Geld bei der Druckerei bestellt.

Referenzen

[1] https://www.stlouisfed.org/open-vault/2019/august/open-market-operations-monetary-policy-tools-explained

[2] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[3] https://fred.stlouisfed.org/series/TREAST

Die Fed zahlt dem Finanzministerium folgende Beträge für “Dollarscheine”:

Nennwert	Preis
1 $	5,5 US-Cent
2 $	5,5 US-Cent
5 $	11,4 US-Cent
10 $	11,1 US-Cent
20 $	11,5 US-Cent
50 $	11,5 US-Cent
100 $	14,2 US-Cent

Hätte das Drucken einer 1-Dollar-Note im Jahr 1915 5,5 Cent gekostet, wären es heute rund 1,40 $. Wenn die Druckkosten einer Banknote ihren Nennwert erreichen, ist sie vom Fiat- zum Warengeld[1] geworden. Bei anhaltender Abwertung muss die Ausgabe des Nennwertes eingestellt werden. Die Beobachtung von Zentralbanken, die sich in einer Hyperinflation[2] befinden, ist aufschlussreich, da Geld die Druckkosten in immer kürzeren Zeiträumen erreicht und Münzen dazu neigen, vollständig zu verschwinden. Die Ausgabe größerer Banknoten ermöglicht es, dass das Geld weiterhin Fiatgeld bleibt, während das Warengeld aufgegeben wird. Der Simbabwe-Dollar[3] erreichte Scheine mit 100.000.000.000.000 Einheiten, bevor er zugunsten ausländischer Währungen vollständig aufgegeben wurde.

Ohne diese Möglichkeit, Fiatgeld zu schaffen, wäre die Fed nicht in der Lage, Konten zu begleichen, genau wie jede Bank, wenn die Reserven (einschließlich der Kreditreserven)

Referenzen

[1] https://de.wikipedia.org/wiki/Primitivgeld

[2] https://en.wikipedia.org/wiki/Hyperinflation_in_Venezuela

[3] https://de.wikipedia.org/wiki/Simbabwe-Dollar

nicht ausreichen, um Abhebungen und Zahlungsausfälle abzudecken. Solange die Mitgliedsbank nicht in Geld abrechnen muss, wie etwa bei Bargeldabhebungen an Geldautomaten[1], Bankschaltern[2] oder bei Nichtmitgliedsbanken und anderen Institutionen, besteht keine Notwendigkeit, das tatsächliche Geld zu bewegen oder zu drucken.

Aber ohne die Möglichkeit, es unter dem Selbstkostenpreis zu drucken, wäre die Fed wie jede andere Bank einem Zahlungsausfall ausgesetzt.

Die Gesamtmenge der im Umlauf[3] befindlichen US-Dollar wird als „M0" bezeichnet. Dazu gehören sämtliche materiellen Zahlungsmittel („Bargeld in Tresoren") sowie immaterielle Bankguthaben auf Konten der Federal Reserve. Diese beiden Formen gelten als austauschbare „Verpflichtungen"[4] (Geld) der Fed. Bei den immateriellen Verbindlichkeiten handelt es sich um Geld, das verbucht, aber noch nicht gedruckt wurde.

Wenn die Kreditaufnahme der Mitgliedsbanken sich verringert, etwa weil die Fed ihre Zinssätze erhöht, können die Verpflichtungen der Fed vernichtet werden, was den gegenteiligen Effekt ihrer Geldschöpfung hat. Zwar hat die Fed M0 in den vier Jahren seit ihrem Höchststand im Jahr 2015 um fast 20 Prozent reduziert[5], doch dies geht zu Lasten der Steuereinnahmen. Die Fed gibt sich als gemeinnützige Organisation aus und überweist jährlich den Nettoertrag aus ihren Krediten an das US-Finanzministerium[6].

Referenzen

[1] https://de.wikipedia.org/wiki/Geldautomat

[2] https://en.wikipedia.org/wiki/Bank_teller

[3] https://en.wikipedia.org/wiki/Money_supply#United_States

[4] https://en.wikipedia.org/wiki/Money_supply#Money_creation_by_commercial_banks

[5] https://tradingeconomics.com/united-states/money-supply-m0

[6] https://www.stlouisfed.org/on-the-economy/2018/september/fed-payments-treasury-rising-interest-rates

Die Federal Reserve hat den Leitzinssatz seit Dezember 2015 bis Juni 2018 sieben Mal erhöht. Dies hat Auswirkungen auf die Entwicklung des Bundesdefizits und der Staatsverschuldung auf zwei Arten:

* Direkt durch Nettozinszahlungen
* Indirekt durch die jährlichen Überweisungen der Fed an das US-Finanzministerium

Die jährlichen Überweisungen an das Finanzministerium sind im Wesentlichen die verbleibenden Einnahmen der Fed nach Abzug der Betriebskosten. Laut Gesetz müssen diese zusätzlichen Einnahmen an das Finanzministerium abgeführt werden.

Die Einnahmen an das Finanzministerium erreichten 2015 mit 97,7 Milliarden Dollar ihren Höhepunkt und sind seitdem stetig gesunken. Im Januar überwies die Fed 80,2 Milliarden Dollar an das Finanzministerium.

Federal Reserve Bank of St. Louis

Diese „übrig gebliebenen Einnahmen der Fed" sind die Einnahmen, die nach Abzug der Betriebskosten durch Kredite in Form von Geld erzielt werden, das das US-Finanzministerium zu Nominalkosten druckt, garantiert durch dessen Monopolschutz[1]. Wie oben gezeigt, leiht sich das Finanzministerium auch Geld zu ermäßigten Zinssätzen, das indirekt von der Fed finanziert wird, und zwar durch die Ausgabe von Staatsanleihen. **Auch wenn kein Geld gedruckt und dann direkt beim Finanzministerium eingezahlt wird, ist das Ergebnis dasselbe.**

Staatliches Monopolgeld[2] wird nicht *ex nihilo* durch Bilanzbetrug der Banken geschaffen. Es wird vom Staat buchstäblich aus alten Blue Jeans[3] erschaffen.

Der Übergang zu einer modernen „bargeldlosen Gesellschaft"[4] impliziert, dass die Zentralbanken die bestehende Form der Verbuchung noch nicht gedruckter Fiat-Währungen beibehalten und alle Abrechnungen einfach intern durchführen. Dadurch

Referenzen

[1] https://en.wikipedia.org/wiki/Counterfeit

[2] Kapitel: Taxonomie des Geldes

[3] https://www.washingtonpost.com/news/wonk/wp/2013/12/16/how-tight-jeans-almost-ruined-americas-money

[4] https://www.nytimes.com/2018/11/21/business/sweden-cashless-society.html

entfallen Druck- und Transportkosten für die Abrechnung und es ist eine vollständige Zensierbarkeit gewährleistet. Ein Exemplar von Fedcoin[1], wie beispielsweise die experimentelle e-Krone[2], wäre erforderlich, damit Menschen elektronisch mit Staatsgeld Transaktionen abwickeln können. Bitcoin dient demselben Zweck, allerdings ohne staatliche Kontrolle über Ausgabe (Mining) oder Bestätigung. Aus diesen Gründen kann man nicht erwarten, dass Bitcoin als Reservewährung[3] (Geld) für staatliche Banken fungiert, da es zwangsläufig der gleichen Entwicklung wie der gescheiterte Goldstandard[4] folgen würde. Bitcoins Wertversprechen[5] liegt in der Vermeidung von staatlichem Geld.

Referenzen

[1] Kapitel: Ziele eines Fedcoin

[2] https://www.riksbank.se/en-gb/payments--cash/e-krona

[3] Kapitel: Fehlschluss der Reservewährung

[4] https://de.wikipedia.org/wiki/Goldstandard

[5] Kapitel: Wertversprechen

MINING

Fehlschluss des ASIC-Monopols

Es gibt eine Theorie, dass der Preis von Bitcoin-ASICs[1] von einem Kartell[2] aus Minern kontrolliert wird, was den Mining-Partnern des Kartells einen unverhältnismäßigen Vorteil verschafft.

Es gibt keinen wirtschaftlichen Unterschied zwischen einem Kartell und einer einzelnen Organisation. Die Veränderung der Organisationsgröße ist ein Ergebnis des freien Marktes, die beobachtet werden kann, da das Kapital nach optimalen Größenvorteilen[3] sucht. Wenn Partner ASICs zu einem Preis erhalten, der eine unter dem Marktwert liegende Kapitalrendite ergibt, handelt es sich um eine interne Subvention zwischen Partnern. Dasselbe gilt für einen Preis, der eine über dem Marktwert liegende Kapitalrendite ergibt, wobei die Subvention in die entgegengesetzte Richtung geht. Daher gibt es keinen Nettovorteil durch solche Rabatte zwischen Partnern.

Die Produktion wird im Allgemeinen auf ein Niveau festgelegt, das eine maximale Rentabilität[4] des Kapitals gewährleisten soll. Die einzige wirtschaftlich vernünftige Möglichkeit für einen Hersteller, den Preis zu erhöhen, besteht darin, die Produktion unter dieses Optimum zu begrenzen. Andernfalls führt ein höherer Preis zu nicht verkauften Lagerbeständen, was zu niedrigeren Nettoerträgen führt. Dies bedeutet, dass die Produktion vom Kartell eingeschränkt werden muss, um den Stückpreis[5] für Nicht-Partner zu erhöhen.

Referenzen

[1] https://de.wikipedia.org/wiki/Anwendungsspezifische_integrierte_Schaltung

[2] https://mises.org/online-book/man-economy-and-state-power-and-market/10-monopoly-and-competition/2-cartels-and-their-consequences

[3] https://de.wikipedia.org/wiki/Größenvorteile

[4] https://de.wikipedia.org/wiki/Rentabilität

[5] https://en.wikipedia.org/wiki/Unit_price

Die Begrenzung der Produktion eröffnet anderen Produzenten die Möglichkeit, Kunden mit einem niedrigeren Grenznutzen[1] für das Produkt zu gewinnen, da diese Kunden sonst nicht bedient würden. Folglich senkt der Wettbewerb den Preis, bis der Markt geräumt ist. Ein freier Markt sucht nach dem Gleichgewichtspreis, der die globale Kapitalrendite (Zinsen) ergibt. Ein aktueller Preis über diesem Niveau steigert die Produktion, ein Preis unter diesem Niveau verringert die Produktion. Der Zinssatz wird durch die Zeitpräferenz[2] bestimmt.

Sofern die Produktion nicht überproportional marktfeindlichen Kräften wie Steuern oder Subventionen ausgesetzt ist, hat jeder die gleiche Chance, Kapital zu beschaffen und in der Produktion zu konkurrieren.

Wenn kein Wettbewerb entsteht, bedeutet dies, dass die Erträge in dieser Branche mindestens den durchschnittlichen Markterträgen entsprechen. Steuern und Subventionen verursachen regionale Verzerrungen, beseitigen aber nicht den Wettbewerb. **Mit anderen Worten, ein Monopolpreis kann nur erreicht werden, wenn der Staat Monopolmacht gewährt.**

Eine verwandte Theorie besagt, dass der Kauf von ASICs von diesem Kartell dessen Hash-Power erhöht. Dies ist auf der Grundlage der obigen Erklärung der monopolistischen Preisgestaltung ungültig. Das Kapital des Produzenten wird in jedem Geschäftszweig oder jeder Investition die gleiche Rendite anstreben. Es gibt keinen Grund zu der Annahme, dass die Rendite bei ASICs unverhältnismäßig sein wird.

Eine verwandte Theorie besagt, dass der Proof-of-Work-Algorithmus von Bitcoin als Konsequenz der vermeintlichen Kartellbildung einen Kartellierungsdruck[3] erzeugt. Wenn die Leute wirklich glauben, dass ASICs überteuert sind, ist die rationale Reaktion,

Referenzen

[1] https://de.wikipedia.org/wiki/Grenznutzen

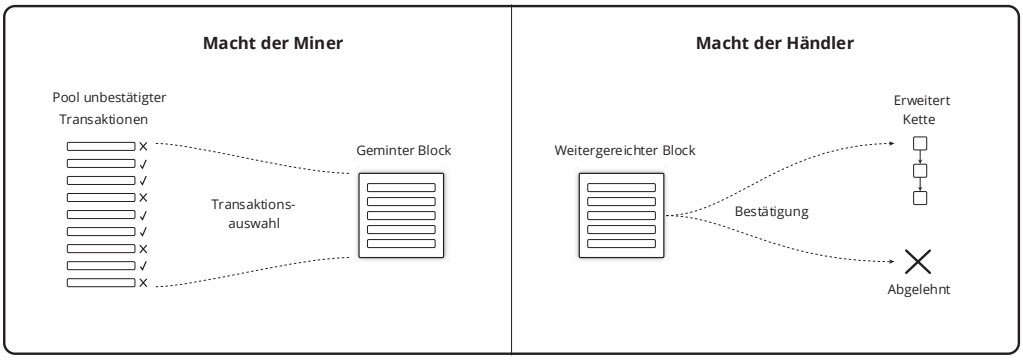
[2] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

[3] Kapitel: Risiko des Kartellierungsdrucks

Kapital zu beschaffen und ASICs herzustellen. Aber in jedem Fall kontrollieren ausschließlich Markt- und marktfeindliche (staatliche) Kräfte die Chipproduktion und stellen daher keinen protokollbasierten Kartellierungsdruck dar.

Fehlschluss des Kräftegleichgewichts

Die Macht in Bitcoin liegt bei Minern und Händlern. Dennoch sind diese beiden Mächte nicht "ausgeglichen", als ob sie in einer Art Checks-and-Balances[1]-System gefangen wären. Die Macht der Miner ist orthogonal[2] zur Macht der Händler. Miner kontrollieren die Auswahl der Transaktionen, Händler kontrollieren die Gültigkeit und keiner kann den anderen kontrollieren. Es überrascht nicht, dass diese Rollen in der ursprünglichen Beschreibung[3] und Implementierung kombiniert waren.



Macht ist nicht dasselbe wie Einfluss. Händler können Miner beeinflussen, indem sie den Service nicht kaufen. Miner können Händler ebenfalls beeinflussen, indem sie ihn nicht anbieten. Diese Entscheidungen manifestieren sich in Splits oder in Stillständen. Es liegt jedoch in der Natur der Macht, dass sie Einfluss ignorieren kann (und dies auch oft tut). Der Staat hat Macht; er kann Zwang und Kooptierung anwenden, während er Einflüsse ignoriert. Händler und Miner *zusammen* haben die Macht, sich gegen diese Aggressionen zu verteidigen[4], aber keiner kann dies ohne die Unterstützung des anderen tun.

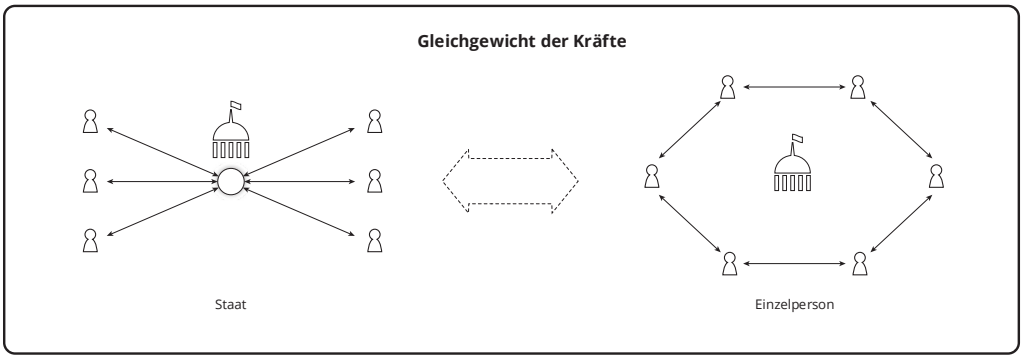
Referenzen

[1] https://de.wikipedia.org/wiki/Gewaltenteilung

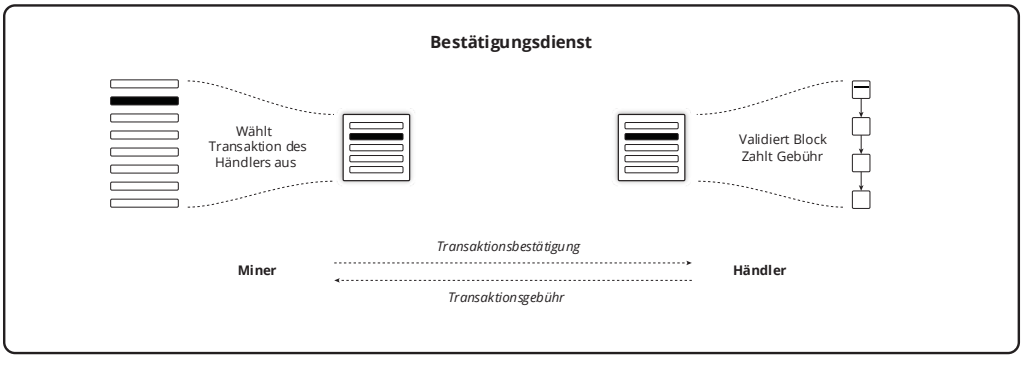
[2] https://de.wikipedia.org/wiki/Orthogonalität

[3] https://bitcoin.org/bitcoin.pdf

[4] Kapitel: Risikoverteilungsprinzip



Das Machtgleichgewicht bei Bitcoin besteht zwischen *Einzelpersonen* und dem Staat. Sogar Staaten schaffen Systeme, welche versuchen[1], ihre Gelder der politischen Kontrolle zu entziehen. Bitcoin ist in dieser Hinsicht nicht anders und berücksichtigt das Widerstandsaxiom[2]. Einzelpersonen können Miner und können Händler sein. Mit einer weiten Verbreitung dieser Aktivitäten wird es für staatliche Akteure schwierig, diesen Markt zu zensieren. **Die Vorstellung, dass sich Miner und Händler in einer konträren Position befinden, ist ein Mangel an Verständnis für das Bitcoin-Sicherheitsmodell.**



Händler erwerben eine Dienstleistung von Minern, und als solche betreiben die beiden Handel. Händler erwerben gegen eine zufriedenstellende Gebühr Mining-

Referenzen

[1] https://www.federalreserve.gov/aboutthefed/bios/board/default.htm

[2] Kapitel: Widerstandsaxiom

Dienstleistungen, die ihren Regeln entsprechen. Es steht ihnen frei, die Blockchain zu spalten und den Minern steht es frei, überhaupt nicht zu minen oder bestimmte Transaktionen aus irgendeinem für sie zutreffenden Grund nicht auszuwählen. Der Handel ist weder kontradiktorisch noch asymmetrisch, er ist freiwillig und für beide Seiten vorteilhaft, wobei alle Spannungen über den Preis gelöst werden.

Der Mangel an Verständnis lässt Menschen glauben, dass Mining zentral gebündelt sein kann, solang die Händler nicht bei der Validierung zentralisiert sind, da die Wirtschaft das Verhalten des Minings kontrollieren und das System sicher machen kann. Dieser Glaube ist falsch, aber leider ziehen die Menschen aus den jüngsten Ereignissen diese ungültige Schlussfolgerung[1]. Ein eng damit verbundener Fehlschluss[2] ist, dass ein Proof-of-Work-Hard-Fork durch Händler das Verhalten der Miner kontrollieren kann.

Referenzen

[1] https://www.coindesk.com/uasf-revisited-will-bitcoins-user-revolt-leave-lasting-legacy

[2] Kapitel: Proof-of-Work-Fehlschluss

Fehlschluss des Mining-Nebenprodukts

Es gibt eine Theorie, dass in dem Maße, in dem beim Bitcoin-Mining ein notwendiges und ansonsten nicht marktfähiges Nebenprodukt[1] der Energieerzeugung, wie etwa ungenutztes Erdgas[2], verbraucht werden kann, eine Verringerung des marktfähigen Energieverbrauchs zu erwarten ist.

Angesichts eines neuen Marktes für Nebenprodukte bedeutet es Opportunitätskosten[3] für jeden Miner, den vermeintlich niedrigeren Preis nicht auszunutzen. Der Wettbewerb um das Nebenprodukt erhöht dessen Preis, bis der Nettovorteil schließlich aufgehoben ist. In der Zwischenzeit stellt dies eine Geschäftschance[4] im Mining dar.

Paradoxerweise[5] führt jede Kostensenkung zu einem proportional höheren Verbrauch. Die reduzierten Kosten des Minings müssen zu erhöhtem Mining führen, damit die Kosten wieder dem Belohnungsniveau entsprechen. Das Nebenprodukt, das früher als Abfall „verbraucht" wurde, erhöht also die Mining-Hash-Rate, bis die gleichen Kosten beim Mining verbraucht werden. Der Nettoenergieverbrauch beim Mining wird durch den niedrigeren Preis tatsächlich erhöht.

Doch durch die Monetisierung einer Abfallressource wird das insgesamt marktfähige Energieangebot erhöht, ohne dass dessen Produktionskosten steigen. Und die Nachfrage nach dem ansonsten marktfähigen Energieangebot im Mining sinkt. Dies bedeutet einen niedrigeren Marktpreis für Energie.

Referenzen

[1] https://en.wikipedia.org/wiki/Waste

[2] https://de.wikipedia.org/wiki/Gasfackel

[3] https://de.wikipedia.org/wiki/Opportunitätskosten

[4] https://bitcoinist.com/bitcoin-mining-waste-oil-industry

[5] Kapitel: Effizienzparadoxon

Eine entsprechende Produktionsausweitung kann im Allgemeinen aus einem reduzierten Energiemarktpreis resultieren. Diese Preisstabilität[1] ist ein allgemeines Merkmal aller Produkte. **Daher kann nicht von einer daraus folgenden Reduzierung des Gesamtenergieverbrauchs durch den Abbau von Nebenprodukten ausgegangen werden**, was die Theorie ungültig macht. Eine allgemeine Steigerung des Wohlstands ist jedoch durch eine höhere Produktion bei gleichen Kosten oder eine gleiche Produktion bei geringeren Kosten impliziert.

Referenzen

[1] Kapitel: Stabilitätseigenschaft

Kausalitätsfehlschluss

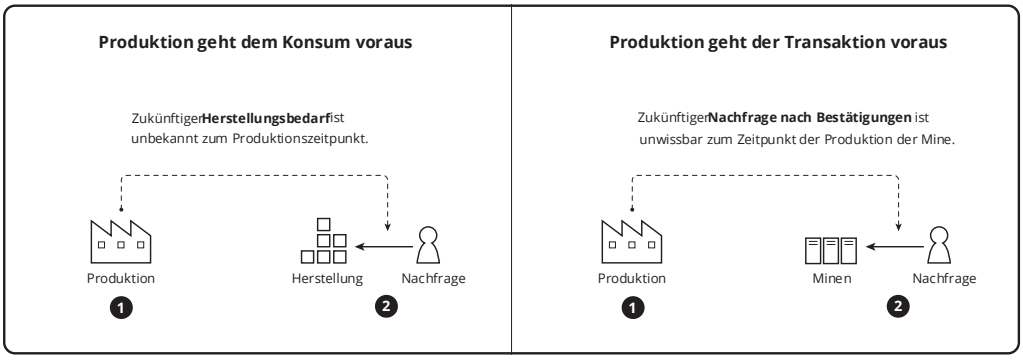
Es gibt eine Theorie, dass das Mining dem Preis, oder genauer, dem Wert der Belohnung „folgt". Die Folgerung ist, dass das Mining dem Preis unterworfen ist und keinerlei Einfluss auf den Nutzen des Coins hat.

Betrachten wir den Miner, der nur auf historische Belohnungswerte reagiert. Diese Person kann nicht der erste Miner sein, da die Belohnung keinen historischen Wert hat. Kein Preis kann festgelegt werden, da keine Geschäfte stattgefunden haben. Der Miner hat vielleicht gehört, dass eine Anzahl unbestätigter Einheiten eine Pizza gekauft hat, aber vielleicht sind dieselben Einheiten doppelt ausgegeben worden. Er muss mit einer bestimmten zukünftigen Nettokapitalrendite rechnen, die erst bekannt ist, wenn sie entweder eintritt oder nicht. Dies ist die Natur des unternehmerischen Risikos. Das Risiko muss eingegangen werden, bevor das Produkt entstehen kann. Man könnte meinen, das Risiko könne durch eine Vorbestellung auf den Verbraucher abgewälzt werden. Doch an diesem Punkt ist der Verbraucher zum Unternehmer geworden, der das Kapital für die Produktion bereitstellt und das Produktionsrisiko übernimmt.

Es ist durchaus möglich, dass ein Miner nur auf historische Belohnungswerte reagiert, wenn die Historie durch die Risikobereitschaft eines anderen festgelegt wurde. Aber welches Zeitfenster und welche Durchschnittsmethode ermöglichen die Vorhersage zukünftiger Belohnungswerte? Die einzigartige Fähigkeit Börsenpreise vorherzusagen, würde dem Miner unbegrenzte Reichtümer bescheren. Wenn dies allgemein möglich wäre, würde sich der Preis nie ändern, da alle möglichen Änderungen bei der ersten Prägung berücksichtigt würden. Der Preis ändert sich also entweder unvorhersehbar oder überhaupt nicht. Mit anderen Worten, jeder Miner ist mit der gleichen Situation konfrontiert wie der erste. Es gibt keine historischen Preise, die zukünftige Preise vorhersagen könnten.

Nimmt man im Allgemeinen eine durchschnittliche Rendite auf dem Markt für Miningkapital an, bedeuten sowohl eine Über- als auch eine Unterschätzung des

Belohnungswerts einen Verlust im Verhältnis zu den Kapitalkosten. Aufgrund der Natur des Wettbewerbs unterliegen Gewinne und Verluste (beziehungsweise Kapitalrenditen über und unter dem Marktwert) einem ständigen negativen Existenzdruck. Mit anderen Worten, der Markt versucht, diese Fehler zu eliminieren. Doch aufgrund der unberechenbaren Natur des Preises gelingt ihm dies nie wirklich. Die Produktion sucht nie nach einer bestehenden Nachfrage, die von Natur aus historisch ist, sondern sie sucht immer nach einer Nachfrage, die sie antizipiert. **Die Produktion prognostiziert weiterhin den zukünftigen Konsum und schafft so die Möglichkeit zum Konsum.**



Miner tauschen ihr Kapital gegen Einheiten von Bitcoin. Dabei machen sie nur einen Bruchteil der Gesamtnachfrage nach Bitcoin aus. Ja, Miner legen den Preis nicht unabhängig fest. Ihre jeweilige Nachfrage hat keinen größeren Einfluss auf den Preis als die eines Nicht-Miners mit der gleichen Nachfrage.

Man könnte sagen, dass Miner sich auf eine Marktrendite für ihr Kapital einigen, indem sie die höchstmöglichen Beträge für Gebühren antizipieren. Aber Händler nähern sich in ähnlicher Weise einer Rendite auf das Miner-Kapital, indem sie den geringstmöglichen Gebührenwert anstreben. Allerdings müssen die Miner die Gesamtnachfrage antizipieren und das Mining-Risiko eingehen, bevor ein Nutzen entstehen kann. Insofern also eine Asymmetrie besteht, geht das Mining der Transaktion voraus, so wie jede Produktion dem Konsum vorausgehen muss. Wenn man etwas anderes annimmt, verwechselt man die Richtung, die ein Markt anstrebt, mit der Art und Weise, in der er dies tut.

Fehlschluss des entkoppelten Minings

Es gibt eine Theorie, dass die Sicherheit[1] durch die Entkopplung der Belohnung von der Transaktionsauswahl beim kartellierten Mining erhöht wird. Die Theorie besagt, dass wenn man nur die Belohnung teilt, die Kontrolle über die Transaktionsauswahl auf Miner mit geringerer Hash-Power übergeht. Das impliziert eine Verringerung des Varianzrabatts[2] und damit eine Steigerung der Wettbewerbsfähigkeit[3] kleiner Minen. Da kleinere Minen vermutlich verdeckter operieren können als größere, bedeutet dies wiederum, dass der Widerstand[4] gegen die Zensur erhöht wird.

Die Theorie berücksichtigt nicht, dass die Kontrolle über die Transaktionsauswahl beim Poolbetreiber verbleibt und ist daher ungültig. Der einzige Vorteil ist die Verringerung der Varianz, die jedoch nur durch den Zahlungseingang erreicht wird. Da die Zahlung nach eigenem Ermessen erfolgt, können beliebige Bedingungen daran geknüpft werden. Solche Bedingungen können Zensur und Identität umfassen. Die Zuflucht eines Mitglieds besteht darin, den Pool für einen anderen zu verlassen, genau wie bei einem gekoppelten Pool. Daher unterliegen entkoppelte Kartelle und gekoppelte Kartelle gleichermaßen der Kooptierung.

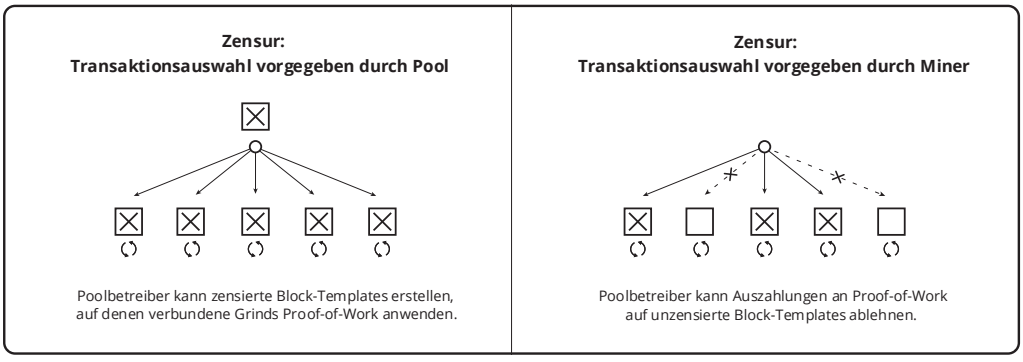
Referenzen

[1] Kapitel: Qualitatives Sicherheitsmodell

[2] Kapitel: Fehler des Varianzrabatts

[3] Kapitel: Eigenschaft der Zensurresistenz

[4] Kapitel: Widerstandsaxiom



Es gibt eine verwandte Theorie, dass die Transparenz eines entkoppelten Pools größer ist als die eines gekoppelten Pools, was die Abwanderung von Mitgliedern zu Pools ohne Zensur erleichtert und somit die Dominanz der Zensurpools begrenzt. Selbst wenn wir die Annahmen größerer Transparenz und unabhängiger Miner, die gegen finanzielle Eigeninteressen handeln, großzügig akzeptieren, bleibt uns immer noch die Tatsache der Kooptierung. Der Staat kann sich immer noch die Möglichkeit vorbehalten, mit den finanziellen Vorteilen der Kartellierung[1] zu operieren und daher ist die Theorie ungültig.

Dieser Trugschluss ähnelt dem Relayfehlschluss[2] insofern als das alle finanziellen Vorteile davon abhängen, dass ansonsten unabhängige Miner die Kontrolle über diesen Vorteil einer einzelnen Person überlassen.

Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

[2] Kapitel: Relayfehlschluss

Dediziertes Kostenprinzip

Unnötige Kosten, die den Minern entstehen, tragen weder zur Doppelausgabenresistenz, noch zur Zensurresistenz[1] bei. Solche Kosten sind echte Verschwendung, sie stellen nichts weiter dar als die Ineffizienz eines bestimmten Miners. So trägt es beispielsweide nicht dazu bei, wenn ein Miner mit falsch konfigurierten Maschinen viel Energie aufwendet und gleichzeitig aufgrund der Fehlkonfiguration keine Belohnung gewinnen kann. Kosten, die nicht unbedingt für die optimale Generierung von Hash-Power erforderlich sind, sind unnötige Kosten. Eine Fehlkonfiguration eines Miners verursacht für einen anderen keine Kosten.

Es gibt eine Theorie, dass Proof-of-Work (PoW) energieeffizienter[2] gestaltet werden kann, indem man der Mining-Funktion nicht dedizierte Kosten hinzufügt. Ein solches Beispiel ist die Entdeckung von Primzahlen[3]. Der Grund für die Einbeziehung solcher Kosten liegt darin, dass die daraus resultierenden Entdeckungen einen mutmaßlichen Marktwert haben. Andernfalls hätte die Einbeziehung objektiv keinen Wert.

Analog dazu können Brauereien ihre Getreidenebenprodukte an Landwirte verkaufen. Das erhöht ihre Effizienz durch Kostenreduzierung. Sofern das resultierende Nebenprodukt also wertvoll ist, verursacht seine Produktion keine Nettokosten. Die notwendigen Nettokosten müssen jedoch aufgrund des Wettbewerbs auf das Niveau der Belohnung steigen. Daher würde dasselbe Ergebnis erreicht, wenn herkömmliches PoW den gesamten Belohnungswert verbrauchen würde und die marktfähigen Produkte von unabhängigen energieverbrauchenden Vorgängen erzeugt würden. **Alle Kosten, die für die Produktion eines unabhängig marktfähigen Wertes aufgewendet werden, können**

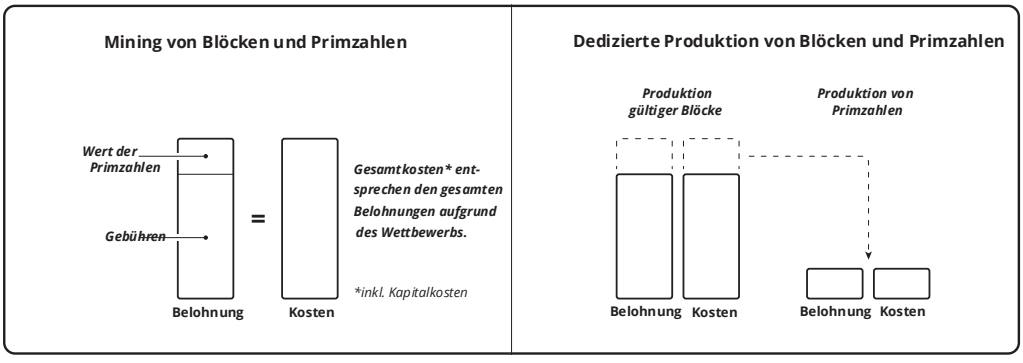
Referenzen

[1] Kapitel: Eigenschaft der Zensurresistenz

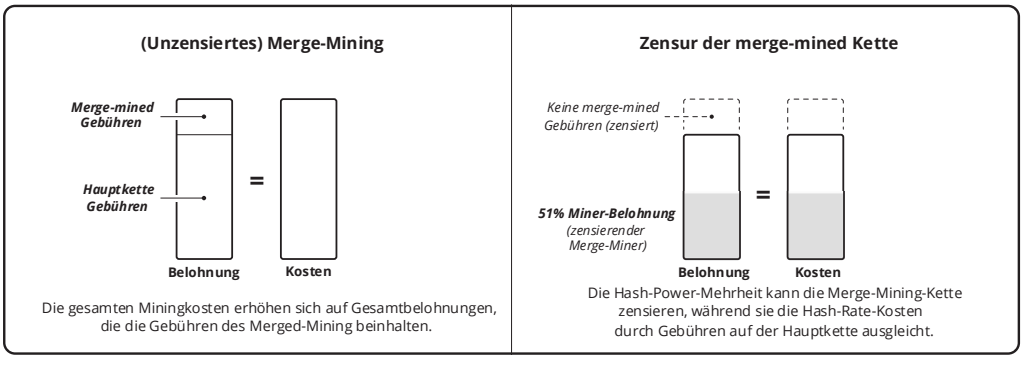
[2] Kapitel: Effizienzparadoxon

[3] http://primecoin.io

durch den Verkauf dieses Nebenprodukts ausgeglichen werden. Daher ist die Theorie ungültig.



Merged Mining[1] wird normalerweise implementiert, um das Problem des Bootstrappings eines neuen Coins über die anfällige Phase der niedrigen Hash Rate hinaus zu lösen. Dieses Design berücksichtigt nicht, dass eine Hash-Rate, die nicht dem neuen Coin gewidmet ist, nicht zu ihrer Sicherheit beiträgt. Da die vollen Kosten der Hash-Rate durch den Verkauf auf einer Blockchain, wieder hereingeholt werden können, entstehen keine Kosten für die Zensur der anderen Merged-Mined-Chain(s).



Referenzen

[1] https://eprint.iacr.org/2017/791.pdf

Effizienzparadoxon

Insgesamt kann das Bitcoin-Mining in Bezug auf die tatsächlichen Kosten nicht effizienter gestaltet werden. Da alle Kosten in Energie aufgelöst werden, könnte man dies auch so umformulieren: Bitcoin kann nicht energieeffizienter gestaltet werden. Paradoxerweise[1] bleiben die Kosten für die Transaktionsbestätigung die Summe der Belohnung für die Bestätigung, egal welche technologische Verbesserung eingeführt wird.

Dieser scheinbare Widerspruch ergibt sich aus der Tatsache, dass die Belohnung letztlich die Kosten bestimmt. Eine Erhöhung der Hash Rate bei gleichen Kosten führt zu einem erhöhten Schwierigkeitsgrad zur Einhaltung der Blockperiode, was die Kosten entsprechend erhöht. Das Bitcoin-Mining muss stets den Betrag der aktuellen Belohnung in Form von Kosten konsumieren.

Referenzen

[1] https://de.wikipedia.org/wiki/Paradoxon

Fehlschluss der leeren Blöcke

Es gibt eine Theorie, dass das Mining leerer Blöcke einen Angriff darstellt. Diese Theorie erfordert nicht, dass die Blöcke auf einem schwachen Zweig gemined werden, um Doppelausgaben zu ermöglichen, noch gibt sie an, welche Person angegriffen wird.

Bedenken Sie Folgendes:

- Der Begriff "Angriff" impliziert Diebstahl. Das Bitcoin-Whitepaper[1] beispielsweise verwendet den Begriff ausschließlich, um Versuche von Doppelausgaben zu beschreiben.
- Eine Belohnung besteht aus Gebühren für Transaktionen und einer Subvention für den Block. Der Miner, der auf Transaktionsgebühren verzichtet, indem er Transaktionen nicht einbezieht, wird für diese nicht belohnt.
- Die Hash-Power des Miners trägt proportional zur Sicherheit des Netzwerks bei. Die Subvention ist eine Entschädigung für diese Sicherheit während der inflationären Phase. Der Zweck der Inflation ist es, Einheiten rational zu verteilen Die rationale Verteilung erfolgt spezifisch im Austausch gegen Hash-Power, nicht für die Einbeziehung von Transaktionen.
- Eine Bestätigung der Transaktion ist nicht garantiert. Gebühren sind der Anreiz für eine Bestätigung. Eine fehlende Bestätigung bedeutet objektiv eine unzureichende Gebühr.
- Das Minen leerer Blöcke ist vollständig konsistent mit den Konsensregeln und kann durch eine neue Regel nicht vernünftig verhindert werden.

Außerdem, wenn 10 % der Hash-Power leere Blöcke minen, dauern Bestätigungen im Durchschnitt 10 % länger. Wenn ein Miner jedoch 10 % der gesamten Hash-Power entfernt, dauern Bestätigungen im Durchschnitt ebenfalls 10 % länger, bis zur nächsten

Referenzen

[1] https://bitcoin.org/bitcoin.pdf

Schwierigkeitsanpassung. Das Mining eines leeren Blocks ist daher nicht vom Nicht-Mining zu unterscheiden.

Es lohnt sich, die Quelle dieses Fehlschlusses zu untersuchen. Aufgrund der Nullsummeneigenschaft[1] könnte man annehmen, dass das Minen eines leeren Blocks "unfairerweise" die Möglichkeit für die Bestätigung von Transaktionen entfernt.

Ein Miner investiert Kapital in Mining und produziert Hash-Power. Lässt man die Effekte der Kartellierung[2] außer Acht, wird der Miner proportional zur Hash-Rate subventioniert. Ohne diese Arbeit würden andere Miner die gleiche durchschnittliche Anzahl von Blöcken mit proportional niedrigerem Schwierigkeitsgrad produzieren. Mit anderen Worten, *tatsächliche* Angriffe wären proportional günstiger. Obwohl der Miner leerer Blöcke also nicht für die Einbeziehung von Transaktionen belohnt wird, sichert er zuvor bestätigte Transaktionen.

Da die Grenzkosten[3] für die Aufnahme einer Transaktion zwangsläufig unter dem durchschnittlichen Gebührenniveau liegen, entstehen dem Empty-Block-Miner Opportunitätskosten[4]. Dies läuft darauf hinaus, dass der Miner die Sicherheit der Blockchain subventioniert.

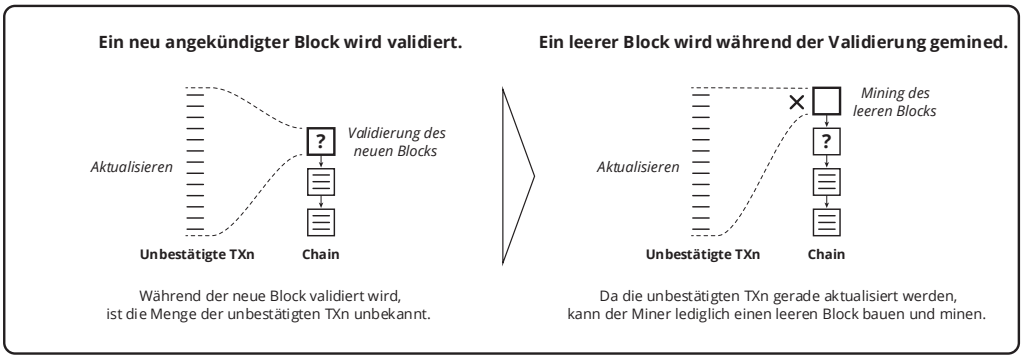
Referenzen

[1] Kapitel: Nullsummeneigenschaft

[2] Kapitel: Risiko des Kartellierungsdrucks

[3] https://de.wikipedia.org/wiki/Grenzkosten

[4] https://de.wikipedia.org/wiki/Opportunitätskosten



Obwohl dies wirtschaftlich irrational erscheint, kann es aufgrund der ausgleichenden Opportunitätskosten für das Warten auf einen neuen nicht leeren Kandidaten nach einer Bekanntmachung auch anders sein. **In dem Maße, in dem es die Kosten der Miner senkt, hat das Empty-Block-Mining keinen Einfluss auf Gebühren oder Bestätigungsraten.** Daher ist die Theorie ungültig.

Während ein bestimmter Miner es für vorteilhaft hält, leere Blöcke zu minen, liegt es in der Macht aller anderen, anders zu handeln. Letztendlich ist es die Ausübung dieser wettbewerbsorientierten und eigennützigen Möglichkeit, die den Coin vor tatsächlichen Angriffen schützt.

Fehlschluss der Energieerschöpfung

Es gibt eine Theorie, dass Proof-of-Work die gesamte den Menschen zur Verfügung stehende Energie verbrauchen könne. PoW wandelt Energie in eine monoton wachsende[1] Barriere für Doppelausgaben für jede beliebige Transaktion um. Dies ist vergleichbar mit der Energie, die aufgewendet wird, um Geld gegen Fälschung zu sichern (durch den eigenen Herausgeber oder anderweitig).

Der Zweck jeder Sicherheitsmaßnahme besteht darin, die zur Überwindung der Maßnahme erforderlichen Kosten, d. h. eine finanzielle Hürde, zu schaffen. Bitcoin schafft diese Doppelausgaben-Barriere, indem es den Angreifer dazu zwingt, den Zweig der anvisierten Transaktion durch einen Zweig mit probabilistisch größerem Aufwand zu ersetzen. Interessanterweise erhöht ein solcher Ersatz die Barriere für nachfolgende Angreifer. **Die aufgewendete Energie ist nicht unabhängig wichtig, die errichtete Barriere ist die notwendige finanzielle Belastung des Angreifers.**

Die Sicherheitsbarriere (S) eines Blocks ist das Produkt der Hash-Kosten pro Einheit (C), der Hash-Rate (H), und der Periode (T).

```
S = C * H * T
```

Die Schwierigkeitsanpassung variiert die Hash-Rate, um eine konstante Periode für gegebene Hash-Kosten und gegebene Sicherheit aufrechtzuerhalten.

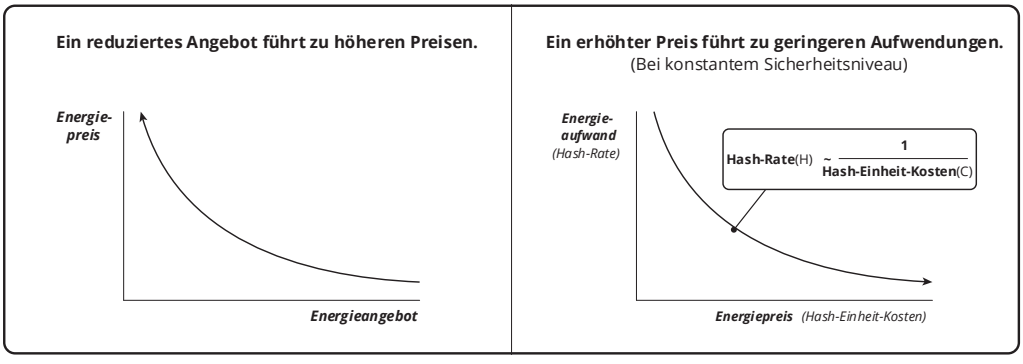
```
T = S / (C * H)
```

Referenzen

[1] https://de.wikipedia.org/wiki/Monotone_Abbildung

Eine konstante Periode impliziert, dass die Hash-Rate umgekehrt proportional zu den Kosten einer gegebenen Sicherheit ist.

```
H ~ S / C
```



Wenn das Energieangebot sinkt, muss der Preis steigen, was den für ein bestimmtes Sicherheitsniveau aufgewendeten Energiebetrag verringert. Daher kann Energie nicht durch Mining erschöpft werden und die Theorie ist ungültig.

Fehlschluss des Energiespeichers

Es gibt eine Theorie, dass der Wert der durch Proof-of-Work aufgewendeten Energie in einen Coinwert umgewandelt wird, wodurch die Energie für den späteren Verbrauch „gespeichert" wird. Unter der Annahme, dass Energie und Coin zu einem späteren Zeitpunkt für Menschen einen Wert haben, können sie wieder zurückgetauscht werden.

Doch das ist bestenfalls eine schlechte Metapher. Miner tauschen Energie gegen Einheiten. Allerdings tauschen *alle* Händler, die Einheiten des Coins annehmen, etwas dafür ein, und *alle Dinge*, die im Handel angeboten werden, stellen die Nachfrage dar. Die Theorie irrt in der Annahme, dass der beim Mining aufgewendete Energiewert einzigartig in seinem Beitrag zum Wert ist. **Abgesehen von der Größe kann eine Nachfragequelle keine allgemein größere Wertdeterminante sein als eine andere.** Daher ist die Theorie ungültig.

Darüber hinaus ist es ein ähnlicher Irrtum zu behaupten, dass Geld[1] ein Wertspeicher[2] ist. Geld ist ein Speicher von Geld. Lediglich Gegenstände können tatsächlich aufbewahrt werden. Der Wert des Geldes leitet sich ausschließlich vom Wert dessen ab, wogegen es die Menschen, die es handeln, eintauschen können. Da Wert subjektiv ist[3], ist er eine menschliche Präferenz, unterliegt ständigen und unvorhersehbaren Veränderungen und kann nicht gespeichert werden.

Referenzen

[1] Kapitel: Taxonomie des Geldes

[2] https://en.wikipedia.org/wiki/Store_of_value

[3] https://en.wikipedia.org/wiki/Subjective_theory_of_value

Fehlschluss der Energieverschwendung

Es gibt eine Theorie, dass Proof-of-Work Energie verschwendet. Dies impliziert, dass das bereitgestellte Sicherheitsniveau höher als nötig ist oder dass dasselbe Sicherheitsniveau durch einen anderen externalisierten Beweis zu geringeren Energiekosten bereitgestellt werden kann. Ein *internalisierter* Beweis, insbesondere Proof-of-Stake[1], ist ein anderes Sicherheitsmodell, das nicht kryptodynamisch sicher[2] ist und hier nicht berücksichtigt wird.

Die gesamte Hash-Power ist eine Funktion der Belohnung, die wiederum eine Funktion der Gebühren ist, die vom Markt für Bestätigungen bestimmt werden. Wenn eine Person die aktuelle Hash-Power als unzureichend erachtet, um den Handel mit einem bestimmten Wert gegen Doppelausgaben abzusichern, erhöht sich die Anforderung an die Tiefe. Darüber hinaus werden, wie in der Eigenschaft der Nutzenschwelle[3] gezeigt, Transaktionen, deren Wert selbst für eine einmalige Bestätigungssicherheit nicht ausreicht, über den Preis aus der Blockchain ausgeschlossen.

Diese oberen und unteren Sicherheitsgrenzen hängen von den Bestätigungskosten ab und sind daher unabhängig von der Beweistechnik. **Es gibt kein notwendiges Sicherheitsniveau, nur eine subjektive Bestätigungstiefe und einen Mindestnutzen.**

Die Bestätigungssicherheit steigt mit den Kosten für die Generierung jedes Blocks. Die Doppelausgabe einer Transaktion erfordert, dass ihr Zweig durch einen mit probabilistisch höheren Kosten ersetzt wird. Die Energiekosten können also nur gesenkt werden, indem für eine bestimmte Bestätigungszeit die gleichen Durchschnittskosten aufgewendet werden, jedoch mit einer geringeren Energiekomponente.

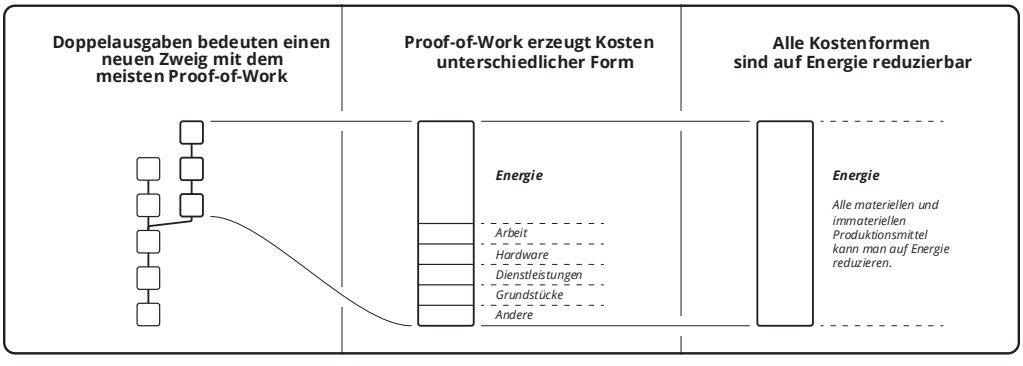
Referenzen

[1] https://de.wikipedia.org/wiki/Proof_of_Stake

[2] Kapitel: Proof-of-Stake-Fehlschluss

[3] Kapitel: Eigenschaft der Nutzenschwelle

Arbeit verursacht Kosten in unterschiedlicher Form, einschließlich Arbeit, Hardware, Dienstleistungen, Grundstücke usw. Jeder andere externalisierte Beweis verbraucht dieselben Ressourcen, wenn auch möglicherweise in einem anderen Verhältnis. Die Frage der Energiekostensenkung reduziert sich daher darauf, ob eine Energiekomponente der Kosten eines Beweises durch eine andere Ressourcenkomponente mit denselben Kosten ersetzt werden kann. Die Kosten der Ersatzressource umfassen jedoch alle ihre Produktionskosten, die in Energie aufgelöst werden müssen. Die Theorie ist daher ungültig.



Darüber hinaus ist die Sicherung jedes Coin für Händler mit Kosten verbunden. Die Tatsache, dass sie sie verwenden, bedeutet daher, dass sie sie gegenüber Alternativen bevorzugen. Dies bedeutet, dass die Alternativen letztlich teurer sind. Da sich alle Kosten grundsätzlich im Energieverbrauch niederschlagen, ist das verwendete Geld[1] das energieeffizienteste.

Referenzen

[1] Kapitel: Taxonomie des Geldes

Fehlschluss der Gebührenrückforderung

Es gibt eine Theorie, dass Miner einen finanziellen Vorteil gegenüber anderen Minern erlangen, indem sie ihre eigenen Transaktionen minen und ihre eigenen Gebühren „zurückerhalten".

Diese Theorie ignoriert die Opportunitätskosten[1] des Minings von Block-Space, ohne eine Zahlung dafür einzuholen. Die Zahlung einer Gebühr *in beliebiger Höhe* an sich selbst ist ein finanzielles Nicht-Ereignis. Das Nichterheben einer Gebühr ist ein echter Kostenfaktor in Höhe des entgangenen Betrags, da die Kosten für das Mining dieses Teils des Blocks nicht kompensiert werden. **Die tatsächlich vom Miner gezahlte Gebühr ist die entgangene Chance.**

Es gibt eine verwandte Theorie, dass Gebührenschätzungstools dazu verleitet werden können, höhere Gebühren zu empfehlen als erforderlich. Wie in Nebengebührfehlschluss[2] gezeigt, wird dabei eine Beziehung zwischen historischen und zukünftigen Gebührensätzen angenommen, die nicht existiert, und dass alle Gebühren in der Blockchain sichtbar sind, was nicht der Fall ist.

Referenzen

[1] https://de.wikipedia.org/wiki/Opportunitätskosten

[2] Kapitel: Nebengebührfehlschluss

Halvingfehlschluss

Bitcoins Konsensregeln erzeugen eine vorhersehbare Inflation. Diese Rate wird regelmäßig an einem Punkt reduziert, den man Halving nennt. Es gibt mehrere Treppenfunktionen[1] in Bitcoin. Das Halving findet alle 210.000 starken Blöcke statt, die Schwierigkeitsanpassung alle 2.016 starken Blöcke und die Organisation der Blockchain ungefähr alle 10 Minuten. Die numerischen Werte, die diese Intervalle steuern, sind beliebig, doch ist die Diskontinuität notwendig, aufgrund der diskreten Intervalle, die für Proof-of-Work erforderlich sind. Es gibt eine Theorie, dass das Halving eine finanzielle Hürde für Miner schafft, die zu einem dauerhaften Stillstand führen kann. Die Theorie basiert auf dem Zusammentreffen zweier Treppenfunktionen (Halving und Schwierigkeitsanpassung), wodurch sich die Periode einer weiteren Treppenfunktion (Organisation) aufgrund der gleichzeitigen Verringerung der Gewinne der Miner dramatisch verlängert.

Die Theorie geht davon aus, dass die Schwierigkeitsanpassung den durchschnittlichen finanziellen Gewinn[2] der Miner auf null zurücksetzt, wodurch nur die obere Hälfte der Miner (nach Rentabilität) überlebt und schließlich nur noch wenige Miner minen. Mit anderen Worten, die Schwierigkeitsanpassung wird als positiver Kartellierungsdruck[3] betrachtet. Es gibt jedoch keinen Grund zu der Annahme, dass die Anpassung den Gewinn *irgendeines* Miners auf null reduziert. Die Konsequenz dieser Annahme ist nicht, dass es nur *wenige* Miner geben wird, sondern dass es allein aufgrund der Schwierigkeitsanpassung *keine* geben wird. Die Anpassung hat eigentlich nichts mit der Regulierung der Gewinne der Miner zu tun, sie kontrolliert nur die Organisationsdauer. Ohne Anpassung wäre der Gewinn unberührt, während die Organisationsdauer und

Referenzen

[1] https://de.wikipedia.org/wiki/Treppenfunktion_(reelle_Funktion)

[2] http://www.investopedia.com/terms/e/economicprofit.asp

[3] Kapitel: Risiko des Kartellierungsdrucks

damit die Varianz auf die gesamte Hash-Rate reagieren würden. Zeitpräferenz[1], die die Kapitalrendite des Marktes vorschreibt, reguliert die Gewinne der Miner, wie sie es in jedem Markt tut.

Betrachten wir den Fall, dass sich der Preis nicht ändert. In diesem Fall gibt es keinen Grund, eine Änderung der gesamten Hash-Rate zu erwarten, keine Anpassungen der Schwierigkeit, und wir können davon ausgehen, dass die durchschnittliche Mine die marktübliche Kapitalrendite erwirtschaftet. Mit anderen Worten, eine beliebige Anzahl unabhängiger Miner kann auf unbestimmte Zeit miteinander konkurrieren (ohne tatsächlichen Kartellierungsdruck).

Man bedenke auch, dass Preisänderungen, Schwierigkeitsanpassungen oder Schwankungen der Belohnung die Profitabilität der Miner auf die gleiche Weise beeinflussen. Eine Schwierigkeitsanpassung und/oder ein Halving ist daher für einen Miner nicht wichtiger als eine vergleichbare Preisschwankung und weist eine größere Vorhersehbarkeit auf.

Die Theorie geht auch davon aus, dass die Belohnung möglicherweise nicht ausreicht, um die Miner für die Schwierigkeit unmittelbar nach einem Halving zu entschädigen. Daher könnten sie sich dafür entscheiden, die Hash-Rate zu senken und die Zeit für Bestätigungen zu verlängern, bis die Gebühren steigen, der Preis steigt und/oder die Schwierigkeit nach unten angepasst wird. Gebühren und Preis werden jedoch auf einem Markt bestimmt und können durchaus auf jedes Niveau steigen, das die Menschen zu zahlen bereit sind.

Es gibt keine Möglichkeit vorherzusagen, welche Niveaus der Markt unterstützen wird, aber der Preis hat weiterhin einen viel größeren Einfluss als Halvings. Die größten Halvings sind ohne Störungen verlaufen. Angesichts der Tatsache, dass

Referenzen

[1] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

nachfolgende Halvings das Äquivalent einer exponentiell *geringeren* Preissenkung bewirken werden, gibt es keinen Grund zu der Annahme, dass zukünftige Ereignisse interessanter sein werden als vergangene.

Fehlschluss des machtlosen Minings

Es gibt eine Theorie, dass Miner keine Macht besitzen. Diese unterscheidet sich vom eng verwandten Proof-of-Work-Fehlschluss[1]. Die Theorie beruht auf der Annahme, dass Miner einem wirtschaftlichen Druck ausgesetzt sind, der anhaltende, effektive Angriffe verhindert. Diese Theorie lässt Menschen glauben, dass das Mining stark kartelliert werden kann, solange die Händler nicht zentralisiert sind, da die Wirtschaft das Verhalten des Minings kontrollieren kann, was das System sicher macht. Die Konsequenz dieser ungültigen Theorie ist Selbstgefälligkeit in Bezug auf die durch Kartellierung verursachte Unsicherheit.

Die Theorie besagt, dass Händler, wenn die Hash-Power-Mehrheit eine Doppelausgabe tätigt, zwangsläufig die Anforderungen an die Tiefe der Bestätigung erhöhen werden, was die Kosten nachfolgender Angriffe erhöht. Irgendwann wird ein Gleichgewicht erreicht, bei dem größere Tiefen als ausreichend für den Austausch angesehen werden. Da dies Doppelausgaben vollständig ausschließen würde, wäre es nicht von Vorteil, den Angriff aufrechtzuerhalten. Die Theorie akzeptiert, dass Angriffe zwar vorkommen können, aber nicht häufig genug, um den Nutzen wesentlich zu verringern.

Die Theorie besagt auch, dass ein Miner nicht darum herumkommen kann, die Transaktionen mit den höchsten Gebühren auszuwählen, da dies die relative Belohnung verringert und andere Miner bereichert. Dies führt mutmaßlich zu einem Verlust der Hash-Power-Mehrheit und damit zu einer Unfähigkeit, fortzufahren. Dieser Aspekt der Theorie impliziert, dass Miner nicht effektiv zensieren können.

Die Theorie geht auch davon aus, dass egoistisches Mining durch die Hash-Power-Mehrheit möglich ist, aber ohne Doppelausgaben und Zensur keine negativen Folgen für die Wirtschaft hat. In diesem Fall wird die Mehrheit einfach zum einzigen Miner, da alle

Referenzen

[1] Kapitel: Proof-of-Work-Fehlschluss

anderen keine Belohnungen behalten können. Trotz fehlender Konkurrenz werden Hash-Rate und Gebührenniveau durch die immer drohende *Möglichkeit* von Konkurrenz aufrechterhalten.

Doch Miner und Händler sind Handelspartner, die sich freiwillig an für beide Seiten vorteilhaften Aktivitäten beteiligen. Wie im Fehlschluss des Kräftegleichgewichts[1] dargelegt, kann keiner den anderen kontrollieren und der Preis ist die Lösung aller Präferenzen. Dies scheint die Theorie zu stützen, **jedoch geht die Theorie nicht auf die Bedrohung ein** und ist in Wirklichkeit eine Nebelkerze[2]. Bitcoin ist so konzipiert, dass es sich gegen nicht marktwirtschaftliche Kräfte, insbesondere den Staat, verteidigen kann. Marktkräfte stellen niemals eine Bedrohung für den Markt selbst dar.

Die Bündelung von Hash-Power untergräbt die Sicherheit, da Staaten sie einfach kooptieren können. Aber Staaten können auch ihre eigenen Minen mit der gleichen Wirkung bauen. Bitcoin erfordert daher sowohl erhebliche Hash-Power *als auch* die Verteilung dieser Power unter Menschen, die bereit und in der Lage sind, staatliche Kontrollen zu riskieren[3].

Der Staat ist ein ökonomisch rationaler Akteur. Inflation ist für den Emittenten profitabel. Die weitverbreitete Nutzung von Bitcoin würde Staaten daran hindern, effektiv eine Inflationssteuer[4] zu erheben. Staatliche Angriffe sind daher zu erwarten, und entsprechende Angriffe sind alltäglich[5]. Es ist praktisch unvermeidlich, dass Staaten Angriffe subventionieren, aber allein die Möglichkeit widerlegt die Theorie.

Referenzen

[1] Kapitel: Fehlschluss des Kräftegleichgewichts

[2] https://de.wikipedia.org/wiki/Red_Herring_(Redewendung)

[3] Kapitel: Risikoverteilungsprinzip

[4] https://de.wikipedia.org/wiki/Seigniorage

[5] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

Miner-Geschäftsmodell

Miner spielen ein Nullsummenspiel[1] innerhalb einer Wirtschaft mit positiven Summen[2]. Sie konkurrieren miteinander, nicht mit der Wirtschaft. Steigender Nutzen ist die Widerspiegelung einer positiven Summe und eine natürliche Folge des Handels.

Es wurde argumentiert, dass Blöcke, die in einer Zeit steigender Preise geschürft werden, den Minern überdurchschnittliche Gewinne einbringen, zumindest bis zur Anpassung der Schwierigkeit. Diese Idee basiert auf dem allgemeinen Unverständnis, dass Marktpreise nicht vorhersagbar[3] sind. Wetten auf Preisänderungen sind spekulativ. Es gibt keinen Grund anzunehmen, dass Bitcoin-Spekulation mehr oder weniger effektiv ist als irgendeine andere. In dem Maße, in dem ein steigender Preis für die Miner im Allgemeinen vorhersehbar ist, sagt die Konkurrenz ihn voraus, was die Idee eines inhärenten überdurchschnittlichen Gewinns entkräftet.

Investitionen in Bitcoin-Mining basieren dagegen auf der vorhersehbaren Beziehung zwischen Gewinn und Wettbewerb im Laufe der Zeit. Diese Beziehung sagt voraus, dass sich der Durchschnitt alles Minings dem Marktzinssatz annähert. Wie bei allen Märkten sind kürzere Zeiträume im Preis unvorhersehbar und längere Zeiträume nähern sich den Marktrenditen an. Letztendlich bestimmt die Zeitpräferenz[4] den Marktzinssatz der Anlagerendite.

Wie also kann ein Miner überdurchschnittliche Gewinne erzielen? Mit Nebengebührenvereinbarungen[5] ist das nicht möglich. Es gibt nur eine Möglichkeit, eine über dem Marktwert liegende Rendite zu erzielen, nämlich unterdurchschnittliche

Referenzen

[1] https://de.wikipedia.org/wiki/Nullsummenspiel

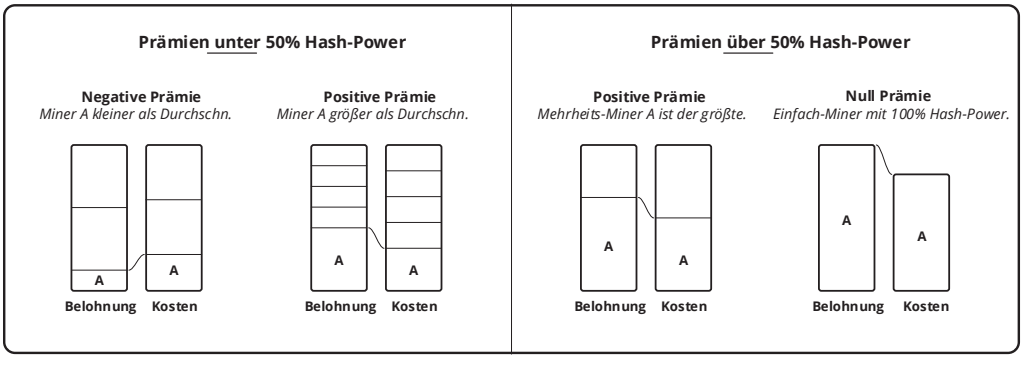
[2] https://de.wikipedia.org/wiki/Win-win

[3] https://de.wikipedia.org/wiki/Chaosforschung

[4] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

[5] Kapitel: Nebengebührfehlschluss

Kosten für die Hash-Power des Coins. Dies wird entweder durch das Ausnutzen des Kartellierungsdrucks[1] oder durch überlegene Betriebseffizienz erreicht. Aufgrund der Nullsummeneigenschaft[2] werden diese durch unter dem Marktwert liegende Renditen anderer Miner ausgeglichen. Die Prämie für einen ehrlichen Miner sinkt daher über 50 % Hash-Power, auf null bei 100 %.



Andere Miner werden jedoch irgendwann aussteigen, da ihr Kapital nach marktüblichen Renditen strebt. Übrig bliebe ein Miner, gebunden an marktübliche Renditen. Mit anderen Worten, um übergroße Renditen zu erzielen, bedarf es anderer, von denen diese Renditen erbeutet werden können. Die höchste nachhaltige Rendite ist eine Funktion der höchsten Opportunitätskosten, die andere bereit sind zu tragen. Dies ist eine Funktion des unterschiedlichen Nutzens der Belohnung, wie im Gefährdungsstufenparadoxon[3] beschrieben.

Indem Dividenden[4] auf die Marktrendite begrenzt und alle verbleibenden Gewinne reinvestiert werden, kann ein Miner eine konstante Hash-Power aufrechterhalten und dadurch Marktrenditen gegen eine Kapitalbasis erzielen, die proportional zur Bitcoin-

Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

[2] Kapitel: Nullsummeneigenschaft

[3] Kapitel: Gefährdungsstufenparadoxon

[4] https://de.wikipedia.org/wiki/Dividende

Kapitalisierung ist. Die Reinvestition von Dividenden erhöht die Hash-Power und die Liquidation verringert sie. Grinds werden liquidiert, indem jedes Gerät offline genommen wird, sobald es zu einem Netto-Minusproduzenten wird, oder indem diese zukünftigen Renditen durch den Verkauf des Gerätes abgezinst[1] werden.

Die Kapitalrendite beim Mining hängt ausschließlich von der Zeitpräferenz ab. Die Beziehung zwischen Wirtschaft und Miningunternehmen wird in Fehlschluss des Kräftegleichgewichts[2] näher untersucht.

Referenzen

[1] https://de.wikipedia.org/wiki/Barwert

[2] Kapitel: Fehlschluss des Kräftegleichgewichts

Risiko des Kartellierungsdrucks

Kartellierungsdruck ist die Summe von finanziellen Anreizen zur Aggregation von Hash-Rate, insbesondere:

- Vorteile der Nähe[1]
- Varianzsrabatt[2]
- Marktvariation
- Marktverzerrung
- Skaleneffekte[3]

Latenz und Varianz sind unvermeidbar. Diese beiden ersten finanziellen Anreize werden tatsächlich durch die Konsensregeln erzeugt. Variation ist eine Folge des schwankenden Marktpreises für Miningressourcen. Marktverzerrung ist eine Folge von nicht marktspezifischen Kosten, einschließlich Steuern, Regulierungen, Subventionen, und Patenten - den Kräften, denen Bitcoin widerstehen[4] soll. In einem Umfeld mit großem Bedrohungspotenzial können sich Skaleneffekte aufgrund der mit der größeren Sichtbarkeit[5] verbundenen Kosten negativ auswirken, ansonsten jedoch positiv sein.

Es gibt verschiedene Erscheinungsformen der Kartellierung. Eine ist geografisch, wobei unabhängige Miner physisch näher zusammenrücken. Eine andere ist kooperativ, wobei ehemals unabhängige Miner ihre Kräfte bündeln und gemeinsam grinden. Eine weitere ist virtuell, wobei Miner zu Grindern werden und die Hash-Rate zu einem einzelnen Remote-Miner zusammenfassen. Eine weitere ist die Verwendung von Relays[6], welche

Referenzen

[1] Kapitel: Fehler der Vorteile der Nähe

[2] Kapitel: Fehler des Varianzrabatts

[3] https://de.wikipedia.org/wiki/Skaleneffekt

[4] Kapitel: Widerstandsaxiom

[5] https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/

[6] Kapitel: Relayfehlschluss

die Hash-Leistung der Miner bündeln. Eine weitere ist der Kapitalfluss, da die mit einer höheren Kapitalauslastung verbundene höhere Hash-Rate eine Form der Co-Location ist.

Unter einem ständigen positiven Druck wird die Transaktionsauswahl letztendlich auf die Kontrolle einer Person reduziert. Es ist möglich, dass das bereits der Fall ist. Das Risiko für Bitcoin besteht darin, dass eine Person der alleinige Verteidiger[1] des Nutzens ist, was eine erfolgreiche Kooptierung unausweichlich macht. Dieses Risiko kann nicht durch die Wirtschaft abgemildert[2] werden.

Kartellierungsdruck ist eine Bitcoin-Analogie zum US-Notenbanksystem[3]. Das System wurde entwickelt[4], um die Besteuerung durch Entwertung[5] eines Marktgeldes zu erleichtern. Es bot staatliche Unterstützung[6] für einen monetären Stellvertreter[7] im Tausch gegen Marktgeld[8]. Diese Kombination sollte Druck erzeugen, um Marktgeld bei einer zentralen Autorität zu sammeln. Sobald diese Einnahmen ausreichten, gab der Staat den Vorwand auf und beschlagnahmte[9] einfach das gesamte verbliebene Marktgeld. Sämtliche Staaten verfügen über ähnliche Systeme und kooperieren[10], um diese zu verteidigen.

Das bedeutet nicht, dass Mining ein Gegenspieler zu Bitcoin ist. Der Analogie folgend ist auch freies Bankwesen[11] kein Gegenspieler zu Gold. Mining ist ein notwendiger

Referenzen

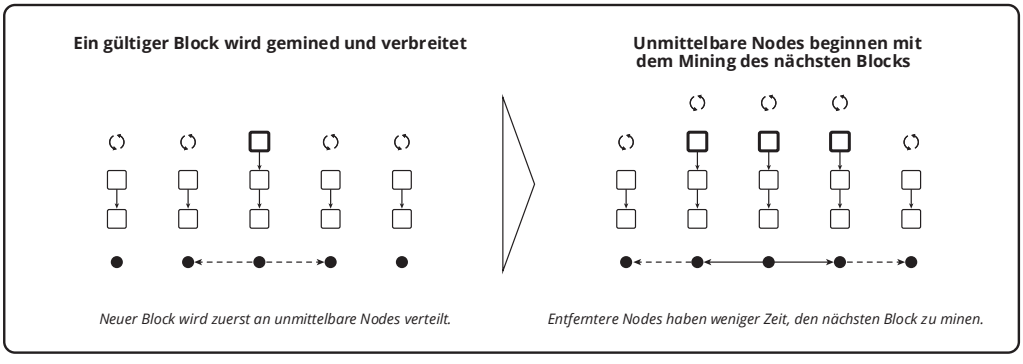
[1] Kapitel: Risikoverteilungsprinzip
[2] Kapitel: Fehlschluss des Kräftegleichgewichts
[3] https://www.federalreserve.gov
[4] Kapitel: Staatsbankenprinzip
[5] https://en.wikipedia.org/wiki/Debasement
[6] https://en.wikipedia.org/wiki/Legal_tender
[7] https://en.wikipedia.org/wiki/Federal_Reserve_Note
[8] Kapitel: Taxonomie des Geldes
[9] https://en.wikipedia.org/wiki/Executive_Order_6102
[10] https://de.wikipedia.org/wiki/Internationaler_Währungsfonds
[11] https://de.wikipedia.org/wiki/Free_Banking

Bestandteil von Bitcoin. Kartellierung stellt ein Risiko dar, allerdings entsteht der Kartellierungsdruck nicht durch die Miner, sondern durch Designfehler in Bitcoin selbst.

Fehler der Vorteile der Nähe

Latenz ist die Zeit, die für Kommunikation erforderlich ist. Informationen bewegen sich mit einer Geschwindigkeit, die nicht größer ist als die Lichtgeschwindigkeit[1], und deshalb kann die Latenz nicht eliminiert werden.

Unterschiedliche Entfernungen zwischen Minern bedeuten, dass einige eher von Bekanntmachungen erfahren als andere. Solange ein Miner nichts von einer Bekanntmachung erfährt, verschwendet er Kapital, indem er an einem schwachen Kandidaten arbeitet. Mit zunehmender Zeit wird es exponentiell unwahrscheinlicher, dass der Miner für den Kandidaten belohnt wird. Miner konkurrieren daher darum, Bekanntmachungen vor anderen Minern zu sehen, da dies die Opportunitätskosten[2] senkt.



Wenn wir Miner mit gleicher Hash-Rate an gleich weit entfernten Punkten auf der Erde verteilen würden, hätten sie die gleiche durchschnittliche Latenz. Aufgrund des finanziellen Vorteils einer geringeren Latenz würden sie jedoch dazu neigen, näher zusammenzurücken. Miner erhalten für die Aggregation eine Prämie auf die Rendite.

Referenzen

[1] https://en.wikipedia.org/wiki/Speed_of_light

[2] https://de.wikipedia.org/wiki/Opportunitätskosten

Dieser auf Nähe basierende Kartellierungsdruck[1] ist eine Folge der linearen Block-Anordnung, die von den Konsenregeln gefordert wird. **Bitcoin schreibt eine „The-Winner-takes-it-all-Ordnung" vor, die unverhältnismäßige Opportunitätskosten erzeugt.** Der Varianzrabatt[2] ist der andere Kartellierungsdruck, der durch Konsens entsteht.

Die Abwehr[3], welche Bitcoin zu verbessern *beabsichtigt*, ist Markt-Abwehr gegen marktfeindliche (staatliche) Kräfte. Um dies zu erreichen, muss die Hash-Power breit unter den Menschen verteilt werden, damit sie nur schwer vereinnahmt werden kann. Der dem Konsens innewohnende Kartellierungsdruck wirkt diesem Ziel jedoch entgegen. Daher wird diese Eigenschaft als Fehler bezeichnet, obwohl noch keine Möglichkeit gefunden wurde, diesen Fehler zu beseitigen.

Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

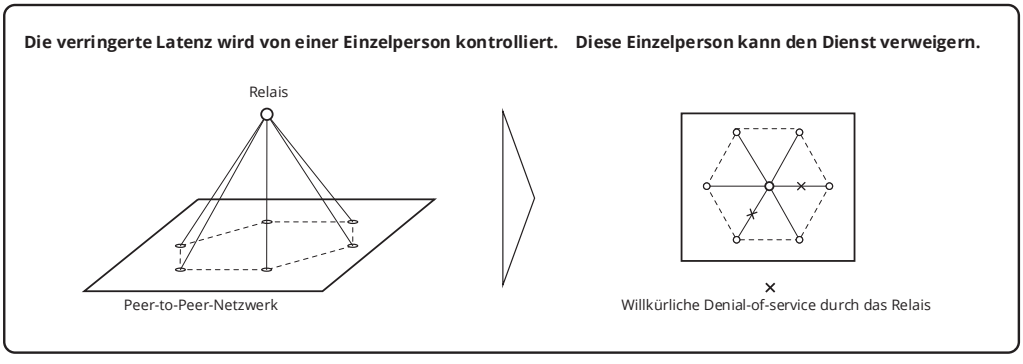
[2] Kapitel: Fehler des Varianzrabatts

[3] Kapitel: Widerstandsaxiom

Relayfehlschluss

Das Peer-to-Peer -Netzwerk verbreitet Blöcke und unbestätigte Transaktionen. Das Protokoll selbst ermöglicht es den Nodes, sich vor Denial of Service-Attacken zu schützen. Für diese Kommunikation ist daher keine Identität erforderlich. Durch diesen Schutz vermeidet das Netzwerk, dass für die Teilnahme eine Erlaubnis erforderlich ist.

Dieser Schutz hat jedoch seinen Preis in Form einer Verzögerung der Bekanntmachung und aufgrund des Vorteils der Nähe[1] führt eine geringere Latenz zu einer höheren scheinbaren Hash-Power. Daher konkurrieren Miner um geringere Latenzzeiten. Eine Möglichkeit, die Latenzzeit zu reduzieren, ist Kartellierung. Eine andere ist die Verwendung eines effizienteren Verteilungsnetzwerks. Da Kartellierung Macht an den Betreiber abgibt, ist vermutlich die letztere Option vorzuziehen.



Eine Möglichkeit, die Verbreitung zu verbessern, ist die *Optimierung* des Peer-to-Peer-Netzwerks. Eine andere Möglichkeit besteht darin, sich einem separaten Netzwerk anzuschließen, das als Relay bezeichnet wird und aufgrund der Beseitigung von Denial-of-Service-Schutzmaßnahmen eine geringere Latenz aufweist, zum Beispiel[2]:

Referenzen

[1] Kapitel: Fehler der Vorteile der Nähe

[2] http://bitcoinfibre.org

> [D]as cmpctblock-Nachrichtenformat wurde so entwickelt, dass es problemlos in einen UDP-FEC-basierten Relay-Mechanismus passt. Der einzige Unterschied besteht darin, dass wir es über UDP mit FEC senden … Auf diese Weise führen zusätzliche Hops nicht zu mehr Latenz. Leider können wir aufgrund der Art unserer FEC-Kodierung nicht wissen, ob einzelne Pakete Teil eines legitimen oder eines beliebigen Blocks sind, und ermöglichen diese Optimierung daher nur zwischen Knoten, die von derselben Gruppe betrieben werden.
>
> *bitcoinfibre.org*

Das Relay akzeptiert Kommunikation einer Gruppe von Minern über das Peer-to-Peer oder ein anderes Protokoll. Das Relay besteht aus seiner Gruppe von Maschinen unter der Kontrolle des Relayers. Es kommuniziert die Bekanntmachungen innerhalb seines internen Netzwerks[1] und schließlich an die angeschlossenen Miner.

Die wichtige Beobachtung hinsichtlich der Sicherheit ist, dass die Kommunikation innerhalb des Relays unter der Kontrolle des Relayers steht. Aufgrund der Entfernung des Denial-of-Service-Schutzes ist für das Schema eine zentrale Kontrolle *erforderlich*. Der Relayer kann bestimmte Blöcke je nach Miner, Region, Signal, Nichtzahlung usw. verzögern. Ein Relayer verkauft reduzierte Latenz und ist daher im Mininggeschäft tätig. Aus Sicherheitsgründen spielt es keine Rolle, ob dieser Service kostenlos angeboten wird. Miner können Grindern in ähnlicher Weise kostenlos reduzierte Latenz Varianz anbieten.

Relays sind Ansammlungen von Minern und Miner sind Ansammlungen von Grindern. Je größer die Hash-Power-Aggregation, desto profitabler ist die Mine und damit auch das Relay. Man kann davon ausgehen, dass Grinder Minen und Miner Relays jederzeit verlassen können und es natürlich möglich ist, dass ein Grinder seine eigene Mine und sein eigenes Relay betreibt. Größere Ansammlungen sind jedoch profitabler, sodass das Verlassen des größten Relays oder der größten Mine die relativen Kosten erhöht[2].

Referenzen

[1] https://bitcoinmagazine.com/articles/blockstream-satellite-broadcasting-bitcoin-space

[2] Kapitel: Nullsummeneigenschaft

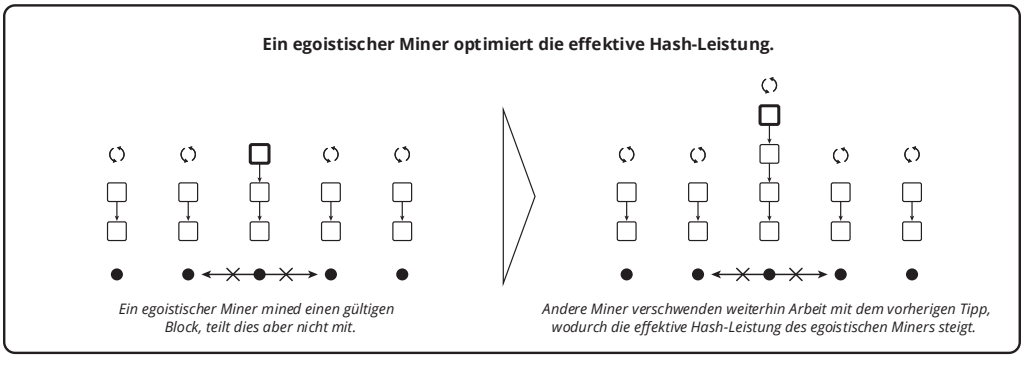
Eine Theorie besagt, dass Relays den Kartellierungsdruck verringern. Das ist ein Irrtum. **Jede durch ein Relay verursachte Verringerung der Kartellierung verschwindet nicht, sondern wird als Erhöhung auf das Relay übertragen.** Relay-Statistiken werden normalerweise nicht zusammen mit Mining-Statistiken präsentiert, wodurch die Machtübertragung verschleiert wird. Dies könnte dazu führen, dass Leute glauben, dass Mining weniger stark kartelliert ist, als es tatsächlich der Fall ist.

Fehlschluss des egoistischen Minings

Der Begriff egoistisches Mining bezieht sich auf eine *Optimierung* des Minings. In einem wissenschaftlichen Artikel[1] wird die Optimierung jedoch folgendermaßen beschrieben:

> Die allgemeine Auffassung geht davon aus, dass das Mining-Protokoll anreizkompatibel und sicher vor kollaborierenden Minderheitengruppen ist, d. h. es bietet den Minern Anreize, das Protokoll wie vorgeschrieben zu befolgen. Wir zeigen, dass das Bitcoin-Mining-Protokoll nicht anreizkompatibel ist.
>
> *Ittay Eyal and Emin Gün Sirer: Majority is not Enough*

Diese Aussage setzt ein „vorgeschriebenes Bitcoin-Mining-Protokoll" voraus, das das Zurückhalten von Bekanntmachungen ausschließt, was jedoch ein Strohmann-Argument[2] ist. Bitcoins Konsensregeln schweigen zwangsläufig zur Zeitsteuerung von Bekanntmachungen.



> Wir stellen einen Angriff vor, mit dem sich kollaborierende Miner einen Gewinn verschaffen, der über ihren fairen Anteil hinausgeht.

Referenzen

[1] https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

[2] https://de.wikipedia.org/wiki/Strohmann-Argument

Diese Aussage setzt ein Konzept des „fairen Anteils“ voraus, welches Bitcoin fremd ist. Ein weiteres Strohmannargument. Ein Miner wird auf der Grundlage der Blöcke belohnt, die ihren Reifegrad erreichen, und nicht als Anteil der tatsächlichen Hash Rate.

Diese Strohmannargumente werden ausdrücklich der „gängigen Meinung“ zugeschrieben. Mit anderen Worten, das Papier verwendet sie, um zu zeigen, dass die gängige Meinung falsch ist. Das Papier irrt sich jedoch, wenn es bedingungslos erklärt, dass dieser angeblich *unfaire Verstoß gegen das Protokoll* einen Angriff darstellt:

> Dieser Angriff kann erhebliche Konsequenzen für Bitcoin haben: Rational denkende Miner werden sich lieber den egoistischen Minern anschließen, und die Gruppe der Komplizen wird immer größer, bis sie die Mehrheit bildet. An diesem Punkt hört das Bitcoin-System auf, eine dezentralisierte Währung zu sein.

Dies ist die Quelle des Irrtums. Falsch zu liegen ist kein Angriff auf die gängige Meinung, es ist ein Fehler in der angenommenen gängigen Meinung. Egoistisches Mining impliziert, dass Bitcoin latenzbasierten Kartellierungsdruck[1] aufweist, obwohl dies ein wohl bekannter Designfehler[2] ist. Jeglicher Kartellierungsdruck neigt dazu, die Anzahl der Miner zu reduzieren, was Bitcoin Angriffen aussetzt.

Optimierungen sind keine Angriffe. Kartellierung erhöht die *Angriffschancen*, aber man sollte diese Chancen nicht mit der Handlung verwechseln. Der Begriff „Angriff“ impliziert Diebstahl. Das Bitcoin-Whitepaper[3] verwendet diesen Begriff lediglich, um Versuche von Doppelausgaben zu beschreiben.

Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

[2] Kapitel: Fehler der Vorteile der Nähe

[3] https://bitcoin.org/bitcoin.pdf

Nebengebührfehlschluss

Es gibt eine Theorie, dass extern gezahlte Gebühren für Transaktionen einen individuellen Anreiz darstellen, dass der Systemsicherheit zuwiderläuft (Anreizinkompatibel[1]). Die Theorie besagt, dass ein Händler, der einen Miner „Off-Chain" für die Bestätigung seiner Transaktionen bezahlt, die Bestätigung der Transaktionen anderer Händler verhindert oder die Kosten dieser Bestätigungen erhöht und so denjenigen einen Vorteil verschafft, die solche Gebühren akzeptieren.

Eine Auswirkung solcher Vereinbarungen ist, dass ein durchschnittlicher *historischer* Gebührensatz nicht durch Analyse der Blockchain ermittelt werden kann. Der scheinbare Satz wäre niedriger als der marktübliche Satz. Das könnte natürlich dazu führen, dass die Geldgeber unterschätzen, was eine ausreichende Gebühr ist. Es gibt jedoch keinen Aspekt von Bitcoin, der erfordert, dass zukünftige Gebühren einem Durchschnitt vergangener Gebühren entsprechen. Schätzungen kompensieren dies zwangsläufig, etwa indem „kostenlose" Transaktionen in vollen Blöcken ignoriert werden oder indem die Standardabweichung[2] zur Identifizierung von Ausreißern verwendet wird. Aber Gebührenschätzungen sind eben nur Schätzungen. Die tatsächlichen Gebührenhöhen werden durch den Wettbewerb gesteuert.

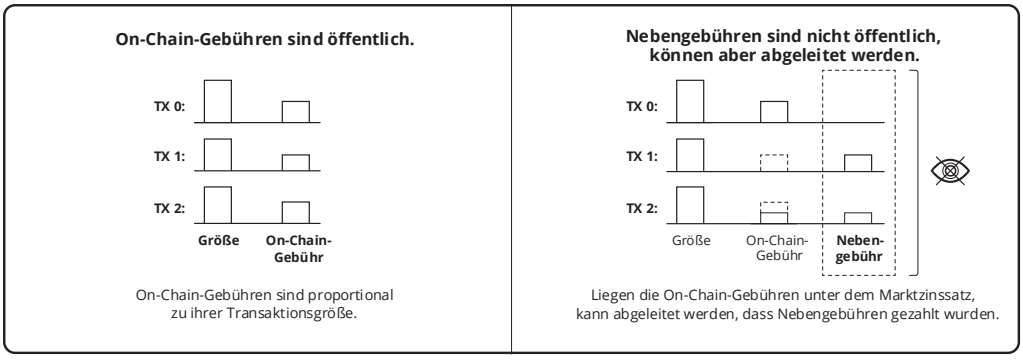
Eine weitere Auswirkung besteht darin, dass unterschiedliche relative Gebührenniveaus darauf hinweisen können, dass bestimmte Transaktionen mit derartigen Vereinbarungen verbunden sind. Dies kann dazu beitragen, die Transaktionen des Händlers und/oder die Coinbase des Miners zu beflecken. Da die Vereinbarung jedoch eine Wahl der Ersteller dieser Transaktionen ist, kommt es zu keinem Verlust der Privatsphäre.

Referenzen

[1] https://de.wikipedia.org/wiki/Anreizkompatibilität

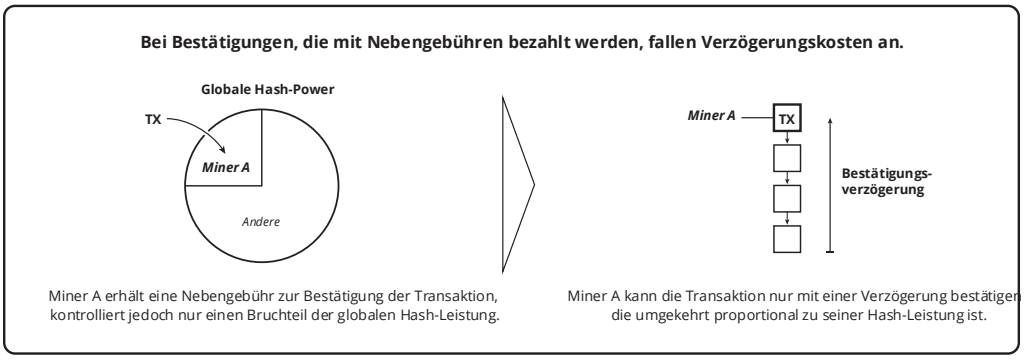
[2] https://de.wikipedia.org/wiki/Varianz_(Stochastik)

Es gibt keine Auswirkungen auf die Marktgebühren oder die Möglichkeit anderer, Bestätigungen zu erhalten. Wenn die Vereinbarung von den Marktpreisen abweicht, akzeptiert entweder der Miner oder der Händler einen unnötigen Verlust. Dies ist nicht anders, als wenn der Miner Transaktionen mit unter dem Marktwert liegenden On-Chain-Gebühren bestätigt oder der Händler die On-Chain-Gebühren überschätzt. In jedem Fall würde die Systemsicherheit nicht beeinträchtigt, selbst wenn alle Gebühren außerhalb der Blockchain gezahlt würden.



Bitcoin bietet einen Mechanismus für On-Chain-Gebühren, sodass eine Transaktion jeden Miner *ohne* Verwendung einer Identität entschädigen kann. Dies ist eine Annehmlichkeit, die die Privatsphäre schützt. **Wenn Miner und Händler es vorziehen, ihre eigene Privatsphäre durch die Ausführung zusätzlicher Aufgaben zu schwächen, gibt es keinen Grund, dies als unerwünscht zu betrachten.** Die Theorie ist daher ungültig.

Darüber hinaus muss der Händler eine verzögerte Bestätigungszeit akzeptieren, die umgekehrt proportional zur Hash-Power des Miners ist. Die Nebengebühr wird zum Marktpreis angeboten, da dem Miner sonst Opportunitätskosten entstehen würden.



Es gibt eine verwandte Theorie, dass Nebengebührenvereinbarungen einen Kartellierungsdruck[1] darstellen. Wenn die gezahlten Gebühren marktkonform sind, kann dies keine Auswirkungen auf die Kartellierung haben. Über dem Marktwert liegende Gebühren sind eine staatliche Subvention, da wir die Subvention als nicht wirtschaftlich rational behandeln müssen. Unter dem Marktwert liegende Gebühren sind eine Steuer, da wir den Verlust als unfreiwillig behandeln müssen. Dies sind Verzerrungen wie bei jeder anderen staatlichen Subvention/Steuer und daher nicht nur bei Nebengebühren zu beobachten. Daher erzeugt die Existenz von Nebengebühren keinen neuen Pooling-Druck, der über den bei On-Chain-Gebühren hinausgeht, und die Theorie ist daher ungültig.

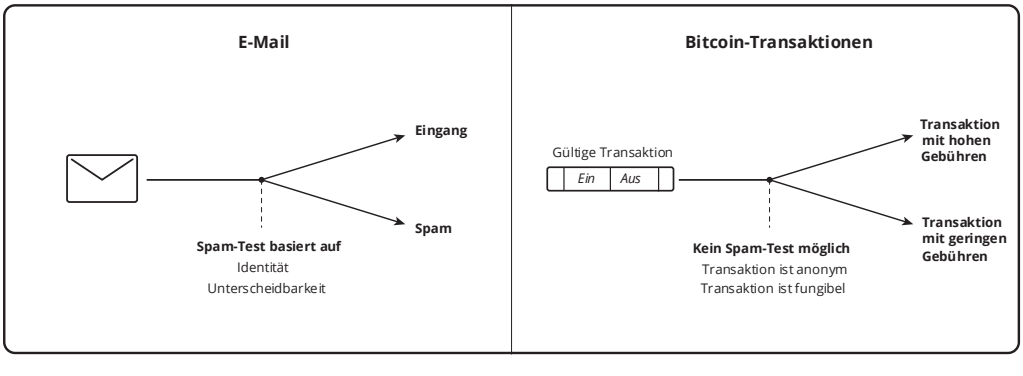
Referenzen

[1] Kapitel: Risiko des Kartellierungsdrucks

Fehlbezeichnung für Spam

Der Begriff Spam[1] bezog sich in der Computertechnik ursprünglich auf exzessives Usenet-Crossposting und wurde später zum Synonym für unerwünschte Broadcast-E-Mails. Obwohl es keine klare Unterscheidung zwischen erwünschten und unerwünschten E-Mails gibt, sind die Nachrichten identitätsbezogen, nicht austauschbar und beinhalten keine Zahlung zur Verarbeitung durch den Empfänger. Bitcoin-Transaktionen sind dagegen zwangsläufig anonym[2], austauschbar und beinhalten eine Zahlung zur Verarbeitung.

Obwohl die Erkennung von E-Mail-Spam ein subjektiver Prozess ist, ist er aufgrund der fehlenden Zahlung für Weiterverarbeitung notwendig. Dieser Prozess wird durch Identität und fehlende Fungibilität erleichtert. Im Gegensatz dazu ist aufgrund der Anonymität und des Fungibilitätsziels kein Test der Legitimation von Transaktionen möglich und aufgrund der Zahlung ist dies auch nicht erforderlich. Mit anderen Worten, **alle gültigen Transaktionen sind gleichermaßen legitim** und dies führt nicht dazu, dass Knoten dem Denial-of-Service-Angriff ausgesetzt werden. Ein korrekter Name für eine Transaktion mit niedriger Gebühr ist „Transaktion mit niedriger Gebühr“.



Referenzen

[1] https://en.wikipedia.org/wiki/History_of_email_spam

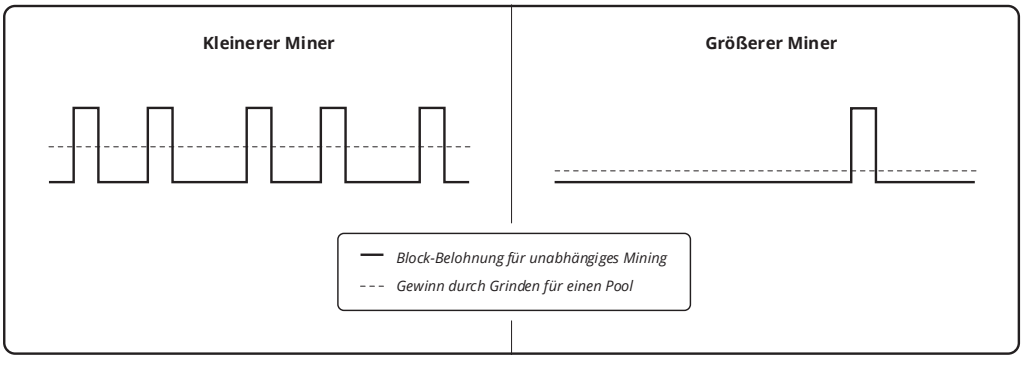
[2] Kapitel: Risikoverteilungsprinzip

Die Übermittlung redundanter Transaktionen in großen Mengen ist ein typisches Denial-of-Service-Problem, das unabhängig von der Transaktionsgebühr ist und von jeder Person, nicht nur vom Ausgebenden, ausgeführt werden kann Bei nicht redundanten Transaktionen mit sich gegenseitig widersprechenden Ausgaben besteht kein Denial-of-Service-Risiko, da sie entweder als ungültig zurückgewiesen oder aufgrund einer ausreichenden Gebührenerhöhung akzeptiert werden.

Fehler des Varianzrabatts

Varianz ist die schwankende Häufigkeit, mit der eine Belohnung erzielt wird. Varianz ist der probabilistischen Natur des Minings inhärent und kann nicht eliminiert werden.

Aufgrund des Konsens impliziert die ungleichmäßige Verteilung der Hash-Power unter Minern , dass manche häufiger Belohnungen erhalten als andere. Mit einer Hash-Rate von 10 % könnte man erwarten, 10-mal häufiger belohnt zu werden als bei 1 %. Die tatsächlichen Ergebnisse sind unvorhersehbar und können erheblich variieren. Aber es reicht in beiden Fällen aus, Proportionalität anzunehmen. In diesem Beispiel erhält ein Miner alle 100 Minuten eine Belohnung und der andere alle 1000 Minuten. Unter der Annahme identischer Belohnungen pro Block ist die Höhe der Belohnung auch proportional zur Hash Power.



Bedenken Sie dann, dass ein kleiner Miner möglicherweise Jahre auf eine Belohnung warten muss. Es besteht auch die Möglichkeit, dass eine Mine falsch konfiguriert ist und nie erfolgreich sein kann. Obwohl ein kleinerer Miner proportional belohnt wird, hat er im Vergleich zu einem größeren Miner ein Defizit. Er muss seinen Cash-Flow[1] verbessern, um häufiger einen Bruchteil der Belohnung zu erhalten. Aus diesen Gründen

Referenzen

[1] https://de.wikipedia.org/wiki/Operating_Cash_Flow

kalkulieren Miner die Renditen für die Varianz ab. Kleinere Miner werden ihre Minen in Grinds umwandeln und einen aggregierenden Miner für eine geringere Varianz bezahlen. Die Vermeidung dieser Aggregation ist die Begründung hinter P2Pool[1], aber da die verteilte Varianzreduzierung weniger effizient ist, dominiert die Kartellierung.

Der varianzbasierte Kartellierungsdruck[2] ist eine Folge der einmaligen Schwierigkeit, wie sie durch die Konsensregeln gefordert wird. **Kleine Miner müssen trotz geringer Hash-Power mit hoher Schwierigkeit konkurrieren, was die inhärente Varianz vergrößert.** Die Prämie für größere Nähe[3] ist der andere Kartellierungsdruck, der durch den Konsens verursacht wird.

Die Abwehr[4], die Bitcoin zu stärken *beabsichtigt*, ist Markt-Abwehr gegen marktfeindliche (staatliche) Kräfte. Um dies zu erreichen, muss die Hash-Power breit unter den Menschen verteilt werden, damit sie nur schwer vereinnahmt werden kann. Der dem Konsens innewohnende Kartellierungsdruck wirkt diesem Ziel jedoch entgegen. Daher wird diese Eigenschaft als Fehler bezeichnet, obwohl noch keine Möglichkeit gefunden wurde, diesen Fehler zu beseitigen.

Referenzen

[1] https://en.bitcoin.it/wiki/P2Pool

[2] Kapitel: Risiko des Kartellierungsdrucks

[3] Kapitel: Fehler der Vorteile der Nähe

[4] Kapitel: Widerstandsaxiom

Nullsummeneigenschaft

Bitcoin-Mining ist ein Nullsummenspiel[1]. Im Durchschnitt wächst die Blockchain alle 10 Minuten um einen Block, wobei die gesamte Belohnung durch ihren Miner kontrolliert wird. Die Miner konkurrieren um diese Belohnung und werden, abgesehen von Kartellierungsdrücken[2], im Durchschnitt jeweils eine Anzahl von Belohnungen erhalten, die proportional zur Hash-Rate ist. Die Differenz zwischen den Kosten eines Miners und dieser Belohnung im Laufe der Zeit ist der Zinssatz für das in der Mine investierte Kapital.

Es gibt zwei Aspekte der Nullsummeneigenschaft:

- Für den Zeitraum zwischen Organisationen erhält ein Miner eine Belohnung und alle anderen Miner erhalten keine Belohnung. Weder Preis, Hash-Rate, Schwierigkeit, Inflation, Gebühren, noch irgendetwas anderes hat irgendeinen Einfluss auf diese Eigenschaft.
- Die Höhe der Belohnungen, entweder in Einheiten von Coins oder im Tauschpreis, hat keinen Einfluss auf die Kapitalrendite.

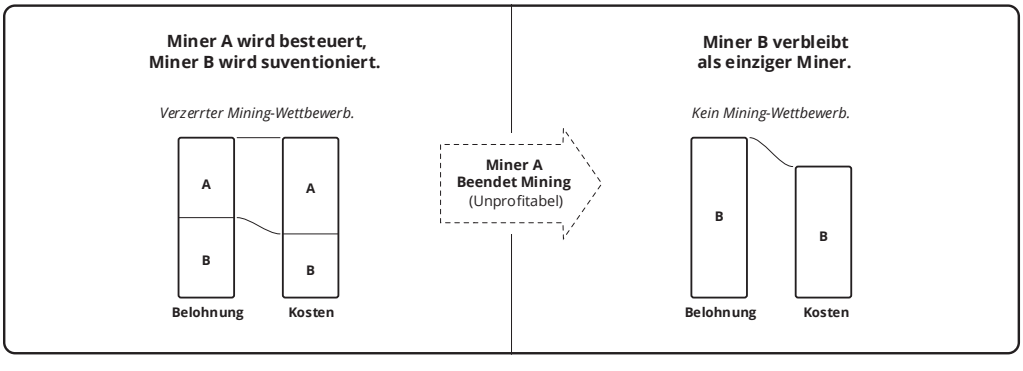
Idealerweise ist Bitcoin-Mining ein geschlossenes System[3]. Die Kapitalrendite variiert im Vergleich zu anderen Minen, sowohl durch die Protokollfehler der Nähenvorteile[4] und des Varianzrabatts[5], als auch durch Skaleneffekte[6] und Betriebseffizienz. **Da sich diese jedoch nur auf die relativen Kosten der Hash-Leistung auswirken, wird die Proportionalität der Rendite beeinträchtigt, nicht jedoch die Gesamtrendite.**

Referenzen

[1] https://de.wikipedia.org/wiki/Nullsummenspiel
[2] Kapitel: Risiko des Kartellierungsdrucks
[3] https://de.wikipedia.org/wiki/Geschlossenes_System
[4] Kapitel: Fehler der Vorteile der Nähe
[5] Kapitel: Fehler des Varianzrabatts
[6] https://de.wikipedia.org/wiki/Größenvorteile

Tatsächlich ist Bitcoin kein geschlossenes System. Der Markt und marktfeindliche Kartellierungdrücke durch Variation und Verzerrung (jeweils) sind extern. Grundsätzlich existiert Bitcoin, um Märkte zu verteidigen, wobei Verzerrung zwangsläufig gegen Variation (oder deren Fehlen) ausgespielt wird.

Wenn in diesem Nullsummensystem eine Verzerrung auf einen Miner angewendet wird, sind alle anderen Miner davon betroffen. Beispielsweise wirkt eine Subvention[1] (nicht zu verwechseln mit einer Konsens-Subvention) für einen Miner wie eine Steuer auf alle anderen, und eine Steuer auf einen Miner wirkt wie eine Subvention auf alle anderen. Der subventionierte Miner arbeitet bei gleicher Hash-Rate zu geringeren Kosten oder hat bei gleichen Kosten eine höhere effektive Hash-Rate (d.h. Hash-Power). Der besteuerte Miner arbeitet bei gleicher Hash-Rate zu höheren Kosten oder hat bei gleichen Kosten eine niedrigere effektive Hash-Rate.



Ein Subventionsgeber erwartet keine Kapitalrendite, sonst würde er als Investor gelten. Investitionen sind eine Marktkraft, bei der der Miner einen Marktpreis für Kapital zahlt. Mit einer höheren effektiven Rendite zieht der subventionierte Miner mehr Kapital an als andere Miner und baut seine Hash-Power weiter aus, bis es einen Miner mit einer Hash-

Referenzen

[1] https://de.wikipedia.org/wiki/Subvention

Power-Mehrheit gibt. Das Ziel des Subventionsgebers ist letztendlich die *Kontrolle* über die subventionierte Mine.

Eine Steuer auf das Mining hat zur Folge, dass Hash-Power in unversteuerte Minen verlagert wird, außerhalb der Reichweite der Steuerbehörde, da das Kapital nach marktüblichen Renditen strebt. Bei breiter Anwendung kann das den Behörden Kontrolle durch ihre eigenen Miningunternehmungen verschaffen. Mit anderen Worten, die Behörde kann den Wettbewerb unterdrücken. Dies kann auch durch eine hundertprozentige Steuer erreicht werden, bei der die Behörde die Minen kooptiert. Die Wirkung ist die gleiche, der besteuerte Miner wird aus dem Geschäft gedrängt und die Steuereinnahmen werden zur Kontrolle eingesetzt.

Die Folgen des Zero-Sum-Minings mit inhärentem Pooling-Druck werden im Gefährdungsstufenparadoxon[1] untersucht.

Referenzen

[1] Kapitel: Gefährdungsstufenparadoxon

ALTERNATIVEN

Bitcoin-Etiketten

Bitcoin hat sich seit seiner Einführung einer klaren Definition widersetzt[1]. Dies ist eine Folge der stark überladenen Verwendung des Begriffs. Der Begriff wurde von Satoshi in Bitcoin: A Peer-to-Peer Electronic Cash System[2] als Bezeichnung für die wesentlichen Konzepte geprägt. Später wurde er auch für die Implementierung des Prototyps, eine Kette (Historie) von Transaktionsbestätigungen, einen Satz von Konsensregeln, die eine Blockchain einschränken, eine Einheit des Coins, und eine vage verbundene Gemeinschaft von Menschen verwendet.

Während es nur einen Satz von Konzepten gibt, gibt es für jeden der anderen Kontexte eine beliebige Anzahl möglicher Variationen, die mit ihnen konsistent sind. Es gibt viele Implementierungen (des Prototyps und andere), Konsensregeln sind abgewichen (beim Prototyp und in anderen Implementierungen), die Geschichte ist dynamisch und willkürlich (selbst der im Prototyp kodierte Genesis-Block hätte ohne Konsequenzen anders sein können) und jeder Coin weist einen unabhängigen Satz von Einheiten auf und wird von ihrem eigenen Satz von Anhängern unterstützt.

Aus diesen Gründen wird Bitcoin hier als Bezeichnung für Kryptodynamische Prinzipien[3] verwendet. Implementierungen werden mit ihren Marken[4] bezeichnet, etwa „Bitcoin Core"[5] oder „Libbitcoin"[6], Blockchains werden mit den allgemein verwendeten Handelssymbolen bezeichnet, etwa „BTC" und „LTC", Konsensregeln für eine bestimmte Blockchain werden im Kontext des Handelssymbols bezeichnet, etwa „LTC-

Referenzen

[1] http://gavinandresen.ninja/a-definition-of-bitcoin

[2] https://bitcoin.org/bitcoin.pdf

[3] Kapitel: Kryptodynamische Prinzipien

[4] Kapitel: Markenarroganz

[5] https://bitcoin.org/en/bitcoin-core

[6] https://libbitcoin.info

Konsensregeln“, eine Coineinheit wird mit den Kleinbuchstaben des Handelssymbols bezeichnet, etwa „btc“ oder „ltc“ (eine Verfeinerung der mehrdeutigen Konvention, „bitcoin“ in Kleinbuchstaben zu verwenden, um sich auf eine Einheit von „BTC“ zu beziehen), und Communities werden entweder als „Bitcoin-Community“ (allgemein) oder „BTC-Community“ (speziell) bezeichnet.).

Während Maximalisten[1] die Verwendung von „Bitcoin“ als konzeptionelle Bezeichnung ablehnen und es stattdessen mit einer Geschichte assoziieren, **wurde der Begriff in Bezug auf eine Reihe von Prinzipien geprägt und ist weiterhin auf sie anwendbar.** Darüber hinaus gibt es mehrere Fälle unabhängiger Blockchains, die sich an diese Prinzipien halten, was die geschichtsbasierte Bezeichnung mehrdeutig macht. Aufgrund dieser Mehrdeutigkeit haben die Menschen normalerweise die Konvention übernommen, sich eindeutig auf Geschichten anhand von Handelssymbolen zu beziehen.

Referenzen

[1] Kapitel: Definition des Maximalismus

Blockchain-Fehlschluss

Es gibt eine Theorie, dass Eigentumsrechte durch unveränderliche Anspruchsaufbewahrung, sowohl gegen Forderungsverlust als auch gegen das Verwahrrisiko[1] gesichert werden können.

Da ein Anspruch selbst kein Eigentum ist, liegt die Kontrolle über das Eigentum beim Treuhänder, gegen den ein Anspruch geltend gemacht wird. Ein Treuhänder hat die Möglichkeit, das Eigentum abzutreten oder einzubehalten und ist daher eine vertrauenswürdige dritte Partei[2]. Die Annullierung eines Anspruchs durch den Verwahrer wird stets durch die Unterschrift des Verwahrers (kryptographisch oder anderweitig) abgeschwächt, wobei die Durchsetzung der Forderung dem Inhaber überlassen bleibt.

Die Theorie besagt, dass die unveränderliche Aufbewahrung des Anspruchs Sicherheit vor dem Verlust des Anspruchs durch seinen Inhaber bietet, da niemand sonst ein Interesse an dem Verlust hätte. Um den Anspruch jedoch einzulösen, muss sein Inhaber dem Verwahrer einen Eigentumsnachweis vorlegen. Dies erfordert, dass der Inhaber das Geheimnis, das diesen Besitz belegt, nicht verliert. Somit wird die Sicherheit des Anspruchs gegen Verlust überhaupt nicht gemindert, es ändert sich lediglich die Form. Die Theorie ist daher auf der Grundlage der Verlustverhütung ungültig.

Das Speichern einer starken Referenz auf den Anspruch kann die Größe und damit die Kosten seines unveränderlichen Speichers reduzieren. Der Anspruch kann die Form eines menschlichen oder maschinellen Vertrags haben und als Einweg-Hash[3] referenziert werden. In beiden Fällen ist die Validierung und Ausführung des Vertrags

Referenzen

[1] Kapitel: Prinzip des Verwahrungsrisikos

[2] https://de.wikipedia.org/wiki/Trusted_Third_Party

[3] https://de.wikipedia.org/wiki/Kryptographische_Hashfunktion

für die Eigentumsübertragung durch den Verwahrer erforderlich. Daher erhöht ein referenzierter Vertragsanspruch das Verlustrisiko um zusätzliche Daten, den Vertrag.

Wie im Prinzip der Risikoteilung[1] gezeigt, sind Menschen immer die Grundlage der Sicherheit. Menschen können kollektiv handeln, um die Unveränderlichkeit einer Währung und damit alle mit der Kontrolle der Währung verbundenen Anspruchsdaten zu schützen.

Ein Treuhänder ist jedoch eine vertrauenswürdige dritte Partei. Unveränderliche Ansprüche mindern in keiner Weise direkte Angriffe gegen oder durch einen Treuhänder. Wenn der Treuhänder der Staat ist oder dessen Kontrolle unterliegt, bietet der Anspruch keine Sicherheit[2] gegen den Austausch von staatlicher Autorität gegen das nachgewiesene Eigentum an irgendeinem Anspruch. Die Theorie ist daher auch aufgrund eines Verwahrungsversagens ungültig.

Bitcoin als Geld[3] ist nicht treuhänderisch (non-custodial). Seine Einheiten stellen keinen Vermögenswert dar, der von einer vertrauenswürdigen dritten Partei gehalten wird. Das Geld wird direkt zwischen Kunde und Händler gehandelt. In diesem Sinne sind *alle Händler* Verwahrer des Wertes von Bitcoin. **Der Blockchain-Irrtum entsteht aus einem Missverständnis des Bitcoin-Sicherheitsmodells, bei dem Sicherheit der Technologie zugeschrieben wird, im Gegensatz zur Verteilung der Händler.** Der Begriff „Blockchain-Technologie“ verstärkt diesen Irrtum und impliziert, dass es in erster Linie die Struktur der Bitcoin-Daten ist, die diese sichert.

Referenzen

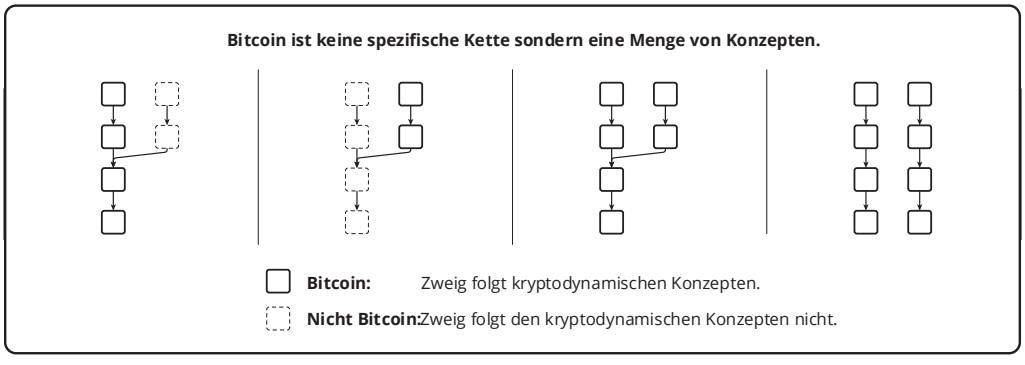
[1] Kapitel: Risikoverteilungsprinzip

[2] https://de.wikipedia.org/wiki/Executive_Order_6102

[3] Kapitel: Taxonomie des Geldes

Markenarroganz

Bitcoin ist ein Satz grundlegender Konzepte[1], keine Blockchain. Niemand kann die Konzepte kontrollieren. Die Menschen werden es verwenden, um eine oder mehrere Blockchains oder Abspaltungen zu beschreiben, während sie sich entwickeln. Das passiert mit allen Geldern[2], einschließlich Gold und Öl, die in unterschiedlicher Reinheit und Qualität gehandelt werden.



Dies steht im Einklang mit der Verkündung von Bitcoin[3], da es sich dabei um eine Reihe von Konzepten handelt, nicht um einen Satz von Regeln, Protokollen, oder Implementierungen. **Menschen mit investiertem Kapital haben ein inhärentes Verlangen nach Markenassoziation, aber es gibt keinen „legitimen" Anspruch darauf.**

Referenzen

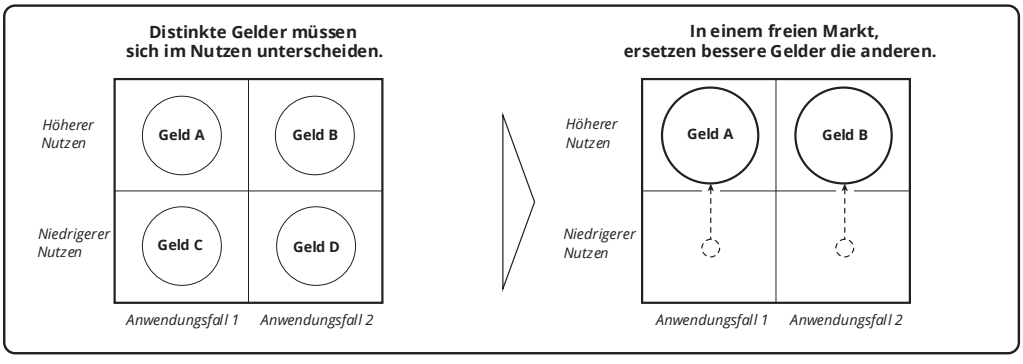
[1] Kapitel: Kryptodynamische Prinzipien

[2] Kapitel: Taxonomie des Geldes

[3] https://bitcoin.org/bitcoin.pdf

Konsolidierungsprinzip

Die Notwendigkeit einen Coin zu wechseln, um mit Händlern eines anderen Coins zu handeln, ist ein Kostenfaktor. Diese Kosten müssen ungleich null sein, auch wenn sie automatisiert sind, da sie Platz und/oder Zeit verbrauchen. Daher ist ein Coin immer „besser" (höherer Nutzen) als zwei, sofern der resultierende Coin nicht gebührenpflichtig ist, wie dies die Eigenschaft der Nutzenschwelle[1] impliziert.



Wir können vernünftigerweise davon ausgehen, dass zwei unterschiedliche Gelder[2] nicht auf Dauer den gleichen Nutzen haben können. Thiers Gesetz[3] erörtert die Folgen von besserem Geld in der Abwesenheit staatlicher Kontrolle. Daraus schließen wir zwangsläufig, dass ohne staatliche Kontrolle **das bessere der beiden Gelder letztendlich das andere ersetzen wird.** Wenn dies geschieht, steigt der Nutzen des überlebenden Coins in umgekehrter Weise wie im Fragmentierungsprinzip[4] beschrieben.

Dies bedeutet nicht, dass keine neuen Coins geschaffen werden können oder über einen längeren Zeitraum existieren. Es bedeutet, dass ein Marktdruck in Richtung eines

Referenzen

[1] Kapitel: Eigenschaft der Nutzenschwelle

[2] Kapitel: Taxonomie des Geldes

[3] https://de.wikipedia.org/wiki/Greshamsches_Gesetz#Umkehrung

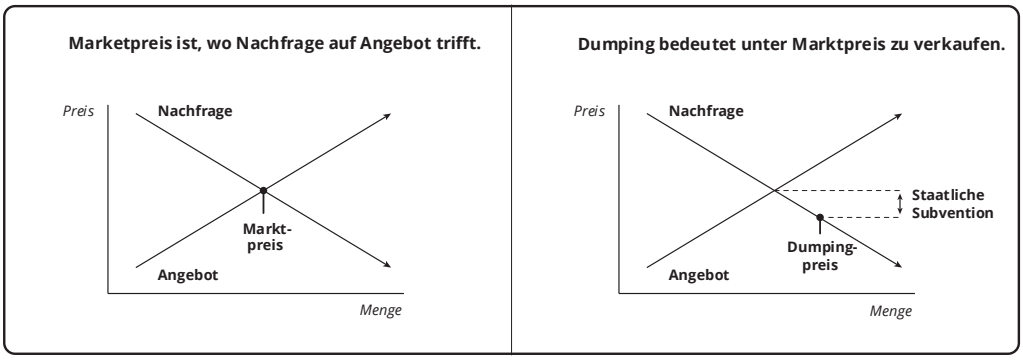
[4] Kapitel: Fragmentierungsprinzip

einzigen Coins besteht. Ein besseres Geld in einer Situation kann in einer anderen Situation nicht besser oder sogar unbrauchbar sein.

Gold ist beispielsweise kein nützliches Zahlungsmittel für den elektronischen Transfer und Bitcoin ist ohne Netzwerk nicht sehr nützlich. Eine Währung ersetzt eine andere in den Szenarien, für die die erstere besser geeignet ist.

Dumping-Fehlschluss

Es gibt eine Theorie, dass der Verkauf von Einheiten von einer Seite eines abgespaltenen Coins für Einheiten der anderen den relativen Nutzen des „verkauften“ Coins verringert. Allerdings verkauft (und kauft) jede Partei. Als ein Handel ist die Aktion symmetrisch und daher ist die Theorie ungültig.



Es gibt eine verwandte Theorie, dass der Tausch von Einheiten einer Seite eines abgespaltenen Coins ein Dumping[1] dieses Coins darstellt, was dessen Nutzen verringert. **Die Theorie stellt das Konzept des Dumpings einfach falsch dar.** Dumping ist staatliche Subventionierung[2] (nicht zu verwechseln mit der Bitcoin-Subvention) eines Produkts, das in einem anderen Staat verkauft wird. Es ist eine Abgabe zulasten der Steuerzahler auf der subventionierenden Seite, typischerweise angewendet, um einen Marktanteil für das Produkt herbeizuführen. Bei elastischer[3] Nachfrage erhöht die Subvention den Absatz des Produkts, indem sie den Preis relativ zum sonstigen Marktpreis senkt. Der niedrigere Preis steigert die Nachfrage, indem er Käufer mit geringerem Grenznutzen[4]

Referenzen

[1] https://de.wikipedia.org/wiki/Dumping

[2] https://de.wikipedia.org/wiki/Subvention

[3] https://de.wikipedia.org/wiki/Preiselastizität

[4] https://de.wikipedia.org/wiki/Grenznutzen

für das Produkt einfängt, bis der Markt sich bereinigt. Im Gegensatz zum Dumping reduziert der Handel zum Marktpreis den Preis nicht, da er nicht subventioniert wird.

Schließlich gibt es noch eine verwandte Theorie, die besagt, dass eine Reduzierung der Hortung[1] generell den Tauschpreis des gehorteten Eigentums senkt. Das ist richtig[2], allerdings ist ein Transfer keine Reduzierung des Hortungsniveaus, es sei denn, der Käufer des gehorteten Eigentums hortet es anschließend weniger als der Verkäufer. Es ist ein Fehler, dies anzunehmen.

Referenzen

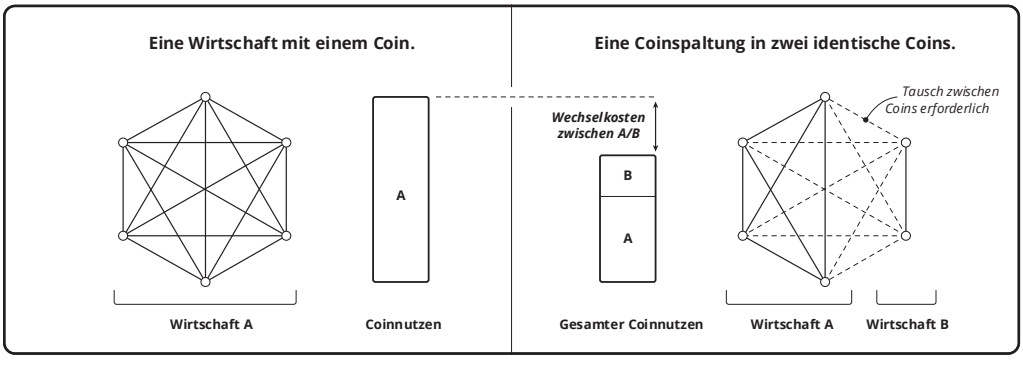
[1] https://en.wikipedia.org/wiki/Hoarding_(economics)

[2] https://mises.org/blog/problem-hoarding

Fragmentierungsprinzip

Der Nutzen eines Geldes[1] leitet sich direkt aus seiner Fähigkeit ab, den Handel zu erleichtern, im Gegensatz zum Tauschhandel[2]. Wenn es von *keinem* Händler akzeptiert wird, hat es objektiv keinen monetären Nutzen. Je mehr Waren und Dienstleistungen[3] (auch unter Berücksichtigung des Standortes) zu einem bestimmten Zeitpunkt mit einer bestimmten Geldmenge gekauft werden können, desto wahrscheinlicher ist es, dass das Geld für eine bestimmte Person einen größeren Nutzen darstellt.

Eine Abspaltung bedeutet, dass null oder mehr Händler den ursprünglichen Coin nicht mehr akzeptieren und null oder mehr damit begonnen haben, den abgespaltenen Coin zu akzeptieren. Eine „saubere“ Spaltung ist ein hypothetisches Szenario, in dem es keine Überschneidung bei der Akzeptanz der beiden Coins durch die Händler gibt und sich die Händlergruppe nicht ändert. Eine saubere Spaltung erzeugt zwei Wirtschaftsräume aus der ursprünglichen Händlergruppe.



Referenzen

[1] Kapitel: Taxonomie des Geldes

[2] https://de.wikipedia.org/wiki/Tauschhandel

[3] https://en.wikipedia.org/wiki/Goods_and_services

Wenn wir davon ausgehen, dass die Coins bis auf die Tatsache der Aufspaltung identisch sind, impliziert das Konsolidierungsprinzip[1], dass der Nutzen der kombinierten Coins der gleiche ist wie der Nutzen des ursprünglichen Coins abzüglich der Wechselkosten. Das Szenario kann um die Überschneidung von Händlern erweitert werden. Dies hat keine Auswirkungen auf den Nutzen des Coins, da dadurch nur die Wechselkosten vom Käufer auf den Verkäufer verlagert werden.

Eine Erhöhung oder Verringerung der Anzahl der Händler, die einen der beiden Coins akzeptieren, ist ein Nettogewinn bzw. -verlust des Gesamtnutzens, da dies die Beseitigung bzw. das Hinzufügen von Umtauschkosten impliziert. Mit anderen Worten, der Effekt ist proportional zu jedem der Coins in der Abspaltung. Dieser Faktor bezieht sich auf die Einzelheiten einer bestimmten Aufteilung, nicht auf die Abspaltung im Allgemeinen.

Eine Aufspaltung führt daher sowohl zu einer Verschiebung als auch zu einer Verringerung des Nutzens, und zwar proportional zur relativen Größe der resultierenden Wirtschaftsräume. Der Fehlschluss des Netzwerkeffekts[2] erklärt, warum die Verringerung nicht quadratischer Natur ist, wie manchmal angenommen wird.

Während es so aussehen mag, als hätte jemand bei der Verschiebung Wert vom ursprünglichen Coin „genommen", ist dieser Wert tatsächlich „weggegangen", um den abgespaltenen Coin zu bilden. Mit anderen Worten, Händler sind Herren des Werts, den sie einer Währung verleihen. Eigentümer haben unabhängigen Einfluss auf die Kaufkraft, basierend auf ihrem Hortungsniveau[3]. Dies wirkt sich jedoch auf den Stückpreis aus, nicht den Nutzen.

Referenzen

[1] Kapitel: Konsolidierungsprinzip

[2] Kapitel: Fehlschluss des Netzwerkeffekts

[3] Kapitel: Dumping-Fehlschluss

Bei der Abspaltung werden aus einer ursprünglichen Einheit zwei Einheiten, von denen jede im Vergleich zur ursprünglichen Einheit einen verringerten und proportionalen Nutzen aufweist. Mit einem bidirektionalen obligatorischen Wiederholungsschutz[1] kann jede Einheit ohne zusätzliche Kosten ausgegeben werden. Andernfalls werden Einheiten der ursprünglichen Blockchain(s) aufgrund der Notwendigkeit des Selbstschutzes abgezinst[2].

Diese Analyse ist auch auf neue Coins anwendbar. Der Unterschied bei einem neuen Coin besteht darin, dass ursprüngliche (andere) Coineinheiten nicht in der neuen Blockchain ausgegeben werden können. Daher steht der neue Coin vor der Schwierigkeit, Einheiten zuzuteilen, was Arbeit und damit Zeit erfordert. Abspaltungen starten[3] diesen Prozess, indem sie den Nutzen einer bestehenden Blockchain unterteilen, sofern ihre Händler dazu bereit sind.

Referenzen

[1] Kapitel: Fehlschluss des Wiederholungsschutzes

[2] https://de.wikipedia.org/wiki/Kapitalwert

[3] https://de.wikipedia.org/wiki/Bootstrapping_(Informatik)

Fehlschluss der genetischen Reinheit

Es gibt eine Theorie, dass ein Coin am stärksten ist, wenn die gesamte Validierung durch eine gemeinsame Implementierung durchgeführt wird. Dieser Theorie zufolge impliziert die Komplexität der Implementierung von Konsensregeln die Wahrscheinlichkeit, dass Implementierungen divergieren, was zu einer unbeabsichtigten Spaltung der Blockchain führt. Die Spaltung impliziert finanzielle Verluste für die Personen auf der schwächeren Seite. Zusätzlich zur Divergenz besteht bei einer einzelnen Implementierung die Gefahr eines globalen Stillstands des Netzwerks. Die Gefahr eines finanziellen Verlusts bedeutet einen geringeren Nutzen und damit eine geringere Systemsicherheit.

Basierend auf der Annahme einer hohen Komplexität, erzeugt jedes Update des "einzig wahren Clients" die gleiche Wahrscheinlichkeit einer Divergenz. Ebenso hat die Abhängigkeit von externen, unabhängig aktualisierten Bibliotheken den gleichen Effekt. Mit anderen Worten, *es ist nicht möglich, dass es nur eine Implementierung gibt*. Im Falle der initialen Bitcoin-Implementierung führten sowohl Upgrades des Clients[1] als auch Upgrades einer externen Abhängigkeit[2] zu unbeabsichtigten Blockchainspaltungen und erheblichen finanziellen Verlusten[3]. Darüber hinaus wurden Zero-Day-Fehler[4] in dieser Implementierung ohne Vorankündigung veröffentlicht[5] und hätten zu einem weltweiten Stillstand führen können.

Referenzen

[1] https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

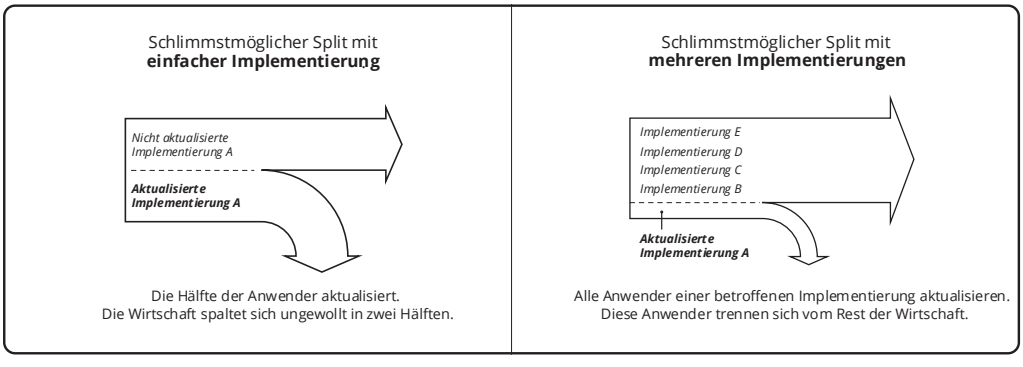
[2] https://github.com/bitcoin/bips/blob/master/bip-0066.mediawiki

[3] https://cointelegraph.com/news/miners-lost-over-50000-from-the-bitcoin-hardfork-last-weekend

[4] https://en.wikipedia.org/wiki/Zero-day_(computing)

[5] https://www.reddit.com/r/btc/comments/6z827o/chris_jeffrey_jj_discloses_bitcoin_attack_vector/

Eine einzelne Implementierung würde eine Schwäche erzeugen, die direkt analog zu der einer lebenden Spezies mit genetischer Einheitlichkeit ist. Im Falle einer einzigen Implementierung dringen sowohl interne als auch externe Updates schnell und tief in die Wirtschaft ein. Die finanziellen Auswirkungen einer Aufspaltung sind daher schwerwiegender als die einer weniger weit verbreiteten Implementierung. In einem Szenario, in dem zehn Implementierungen jeweils einen gleichmäßigen Anteil der Wirtschaft unterstützen, wären bei jedem Update höchstens 10 % der Wirtschaft gefährdet, während das Update einer einzigen universell eingesetzten Implementierung das maximale Aufspaltungsrisiko von 50 % erreicht. Die Theorie ist daher nicht nur ungültig, sondern drückt das Gegenteil des tatsächlichen Verhaltens aus.



Fehlschluss des hybriden Minings

Es gibt eine Theorie, dass eine Kombination aus Proof-of-Work- (PoW) und Proof-of-Stake- (PoS)-Mining ein höheres Maß an Systemsicherheit biete als PoW allein. Die Theorie impliziert, dass eine Mehrheit der Eigentümer der Coins „Fehlverhalten" durch PoW-Miner abmildern kann.

In Ermangelung eines Miners mit der Mehrheit der Hash-Power gibt es nichts abzumildern. Daher basiert die Theorie darauf, die Kosten eines Zensurregiemes zu erhöhen. Dies wiederum beruht auf der unhaltbaren Annahme, dass PoW-Miner nicht auch PoS-Miner sind.

Die Kosten des hybriden Minings sind die kombinierten Kosten für Arbeit und Staking, einschließlich der Kapitalkosten. Die Rendite der Investition für das Mining entspricht aufgrund des Wettbewerbs zwangsläufig den Kapitalkosten. Da Mining profitabel ist, tragen die Kapitalkosten nicht zur Sicherheit bei. **Eine Mehrheitsbeteiligung zu erreichen ist nicht teurer als die Mehrheit der Hash-Power zu erreichen.** Die Theorie ist daher ungültig.

In einem Modell, in dem ein Mehrheitsaktionär die Bestätigung ansonsten gültiger PoW-Blöcke verhindern kann, kann der Zensor nach der Erreichung der Mehrheit nicht mehr abgesetzt werden[1]. Ein solches System ist im Grunde ein PoS-Coin ohne Zensurresistenz[2], wobei der PoW-Aspekt keinerlei zusätzliche Sicherheit bietet.

Referenzen

[1] Kapitel: Proof-of-Stake-Fehlschluss

[2] Kapitel: Eigenschaft der Zensurresistenz

Definition des Maximalismus

Maximalismus ist eine PR-Maßnahme, die die Bildung von Ersatzcoins für einen bestimmten Coin verhindern soll. Sofern das gelingt, kann es bestehenden Eigentümern zugutekommen, indem es das Angebot einschränkt und den Preis erhöht. Da es den Menschen jedoch nicht gelingt, einen annähernden Ersatz[1] zu finden, verlagert sich die Aktivität auf weiter entfernte. Im Fall elektronischer Zahlungen handelt es sich dabei in der Regel um staatliches Geld.

Maximalismus unterscheidet sich von Shitcoin[2]-Bewusstsein insofern, als dass er sich durch die Reklame für einen einzigen Bitcoin gegenüber allen anderen Coins auszeichnet. Befürworter äußern oft die widersprüchliche Theorie, dass kein anderer Coin mit ihrem bevorzugten Coin konkurrieren könne. Wäre dies der Fall, gäbe es keinen Grund, sich für einen einzelnen Coin einzusetzen.

Referenzen

[1] Kapitel: Substitutionsprinzip

[2] Kapitel: Definition von Shitcoin

Fehlschluss des Netzwerkeffekts

Es gibt eine Theorie, dass der von einer Wirtschaft erzeugte Nutzen mit dem Quadrat der Anzahl seiner Händler variiert, vorausgesetzt, dass jeder Händler den gleichen Wert an Waren oder Dienstleistungen in diesem einen Coin zum Verkauf anbietet. Die Theorie ist eine Anwendung des Metcalfeschen Gesetzes[1].

Das bedeutet, dass eine gleichmäßige Aufteilung der Wirtschaft den Gesamtnutzen um die Hälfte reduziert. Wenn beispielsweise ein Netzwerk aus 20 Händlern einen Nutzen von 400 hat, dann haben zwei Netzwerke aus jeweils 10 dieser Händler einen Nutzen von 200.

Die Möglichkeit, beliebige Einheiten eines Coins gegen eine andere auszutauschen, lässt jedoch den Nutzen der beiden Volkswirtschaften zu einer Hybridwirtschaft zusammenfallen. Aufgrund der Umtauschkosten[2] **hat der Hybridcoin einen geringeren Nutzen als ein einzelner Coin, aber dies ist nicht vergleichbar mit dem vollständigen Verlust eines der beiden, es sei denn, die Umtauschkosten sind unbegrenzt.** Die Theorie ist daher ungültig.

Referenzen

[1] https://de.wikipedia.org/wiki/Metcalfesches_Gesetz

[2] Kapitel: Konsolidierungsprinzip

Fehlschluss des Kostennachweises

In einem wettbewerbsorientierten (freien) Markt kostet das Bitcoin-Mining dem Miner so viel, wie es ihm an Wert verschafft, sowohl durch die Emission neuer Einheiten als auch die Dienstleistung der Bestätigung. Dies gilt unabhängig davon, ob die Belohnung für den geschürften Block die volle Rendite des Miners widerspiegelt oder nicht.

Der Rechenaufwand beim Mining spiegelt sich probabilistisch in der Block-Schwierigkeit wider. Diese Berechnung nennt an Arbeit. Ein gültiger Block-Header ist ein probabilistischer Beweis dafür, dass diese Arbeit geleistet wurde. Dies ist die Grundlage des Begriffs „Proof of Work".

Die bei der Blockproduktion verbrauchte Energiemenge kann weder konkret noch probabilistisch nachgewiesen werden. Die Energieeffizienz variiert. Ein Blockheader stellt keinen „Nachweis der verbrauchten Energie" dar. Solche Angaben sind Näherungswerte.

Die Rendite eines Miners aus der Blockproduktion wird nicht vollständig durch den Block widergespiegelt. Das Mining der eigenen Transaktionen bringt Gebühren mit sich, die sich nicht unbedingt im Block widerspiegeln, wie dies bei Nebengebühren[1] im Allgemeinen der Fall ist. Ein Miner kann Transaktionen mit beliebig hohen oder niedrigen Gebühren einführen. Die Blockbelohnung stellt keinen „Beweis für die Belohnung" dar. Solche Behauptungen sind Annahmen.

In einem freien Markt ist die Rendite beim Mining der Wert der Belohnung, unabhängig davon, ob der Betrag im Block wiedergegeben wird oder nicht, und die verdienten Gebühren werden durch die Transaktionsnachfrage bestimmt. Dies ist eine Folge des Wettbewerbs. In diesem Fall ist es also richtig, einen gültigen Blockheader als

Referenzen

[1] Kapitel: Nebengebührfehlschluss

„Kostennachweis“ zu betrachten, die Höhe der Kosten bleibt jedoch unbekannt. Alles, was bekannt ist, ist, dass der Miner eine marktübliche Kapitalrendite erzielt hat.

Bei einem staatlichen Monopol[1] wird der Preis jedoch nicht durch den Wettbewerb kontrolliert. Ein Monopol kann jeden Preis verlangen, den der Markt hergibt. Die Kosten für die Durchsetzung des Monopols trägt der Steuerzahler. Der Preisaufschlag ist eine weitere Steuer, die vom Verbraucher gezahlt wird. Der Wert der Steuer wird auf das Monopol übertragen.

Im Falle der staatlich geförderten Bitcoin-Zensur existieren sowohl die Durchsetzung als auch der Preis-(Gebühren-)Aufschlag als Steuern im Sinne eines Monopols. Die Höhe der Gebühr kann den Marktpreis übersteigen und ihre Durchsetzung wird durch Steuern subventioniert. Monopol-Mining kann Seigniorage[2] erzeugen, genau wie jedes Monopolgeld. Der Blockheader liefert weiterhin einen Arbeitsnachweis, aber keinen Nachweis der Marktkosten mehr.

In gleicher Weise liefert die Existenz einer gültigen Einheit Monopolgeldes[3] einen ausreichenden Beweis für die tatsächlichen Produktionskosten, aber keinen Beweis dafür, dass der Emittent keine Monopolprämie auf diese Kosten verdient hat. Es gibt eine Theorie, dass die Produktionskosten von Bitcoin „fälschungssicher“ sind, wobei die Seigniorage von Staatsgeld eine „Kostenfälschung“ darstellt. Wie gezeigt wurde, **unterliegt Bitcoin ebenfalls der Seigniorage**, was die Theorie entkräftet.

Referenzen

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/pp/1054

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] Kapitel: Taxonomie des Geldes

Alle Waren haben reale Produktionskosten. Monopole existieren, um die Preise über die Kosten zu treiben. Bitcoin ist zwar zensurresistent[1], die Wirksamkeit der Zensurresistenz ist jedoch nicht garantiert[2].

Referenzen

[1] Kapitel: Eigenschaft der Zensurresistenz

[2] Kapitel: Widerstandsaxiom

Proof-of-Memory-Fassade

Es wurde vorgeschlagen[1], dass ein Proof-of-Memory (PoM) einen Teil der Energiekosten eines Proof-of-Work (PoW) durch Hardware ersetzen kann, selbst wenn vorhandene Speichergeräte verwendet werden. Wie im Fehlschluss der Energieverschwendung[2] gezeigt, erfordert ein konstantes Sicherheitsniveau konstante laufende Ausgaben. Daher würde ein solches System einen vergleichbaren Hardwareverbrauch erfordern, um eine Reduzierung der Energiekosten auszugleichen. **Mit anderen Worten, der Gesamtenergieverbrauch kann nicht reduziert werden, er kann nur auf die Herstellung, den Betrieb und die Entsorgung der Hardware übertragen werden.**

Im Dezember 2017 betrugen die geschätzten jährlichen Kosten für den Energieverbrauch beim Bitcoin-Mining 1.628.000.000 US-Dollar, basierend auf den Schätzungen von 32,56 Terawattstunden, die bei durchschnittlichen Energiekosten von 0,05 US-Dollar pro Kilowattstunde verbraucht wurden. Gleichzeitig entspricht dieser Kostenwert dem Verbrauch von 32.560.000 Terabyte-Laufwerken bei einem durchschnittlichen Preis von 50 US-Dollar pro Laufwerk. Die Nutzung des vorhandenen, nicht ausgelasteten Speichers reduziert die Stückkosten und erhöht daher vergleichsweise den Größenbedarf.

Es lohnt sich, das wirtschaftliche Verhalten eines theoretischen Systems zu betrachten, in dem PoM durch einen vorhandenen (kostenlosen) festen Speicherpool ohne Ablauf- oder Betriebskosten bestimmt wird. Da die Kosten des Minings null sind, fließen Belohnungen ohne Kosten proportional zum Speicher (unter der Annahme, dass kein Kartellierungsdruck[3] besteht). Jede Erhöhung der durchschnittlichen Gebühr erhöht diese Belohnung für den Speicher. Das investierte Kapital ist null und daher ist der

Referenzen

[1] https://eprint.iacr.org/2017/893.pdf

[2] Kapitel: Fehlschluss der Energieverschwendung

[3] Kapitel: Risiko des Kartellierungsdrucks

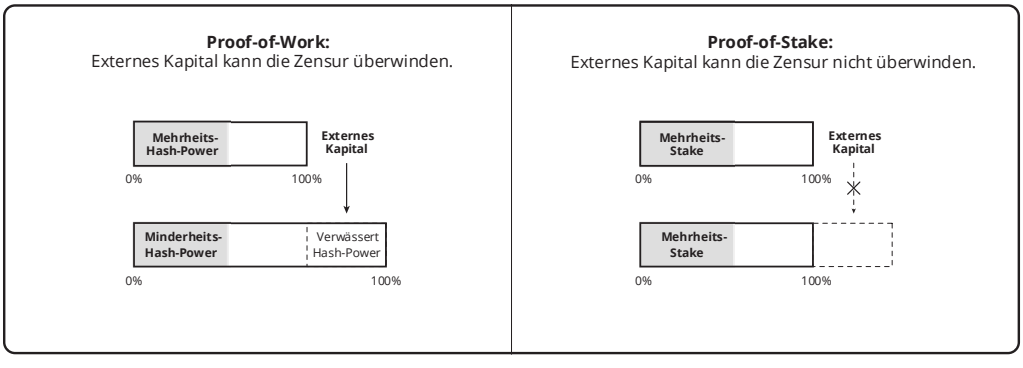
Zinssatz dauerhaft unendlich. Trotz unbegrenzter Anreize schließt die Annahme einer Nullexpansion Wettbewerb aus. Da der Beweis aber externalisiert ist, kann der Wettbewerb genau genommen nicht eingeschränkt werden. In einem realen System expandiert die Hardware-Herstellung bei einem gegebenen Gebührenniveau ständig, und diese Expansion beschleunigt sich mit steigenden Gebühren.

Proof-of-Memory ist in Bezug auf den Ressourcenverbrauch mit Proof-of-Work identisch und es gibt keinen Grund, einen geringeren Energieanteil dieser Kosten anzunehmen. Die Hardware fungiert als Beweisbatterie und stellt nachweislich die bei ihrer Herstellung verbrauchte Energie dar. Dies ist eine Fassade analog zum „emissionsfreien" batteriebetriebenen Auto.

Proof-of-Stake-Fehlschluss

Bestätigungssicherheit erfordert eine autorisierte Person , die Transaktionen aufreiht. Bitcoin weist diese Autorität regelmäßig dem Miner zu, der den größten Nachweis für geleistete Arbeit erbringt. Alle Formen von Arbeit reduzieren sich zwangsläufig[1] auf Energieverbrauch[2]. Es ist unerlässlich[3], dass ein solcher Nachweis unabhängig von der Blockchainhistorie ist. Wir können dies als „externen“ Nachweis bezeichnen.

Die einzige andere Quelle der Anordnungsautorität hängt daher von der Blockchainhistorie ab, die wir als „intern“ bezeichnen können. Es gibt eine Theorie, dass ein solcher Proof-of-Stake (PoS) in Bezug auf die Bestätigungssicherheit eine vergleichbare Alternative zu Proof-of-Work (PoW) darstellt. Es ist wahr, dass sowohl PoS wie auch PoW die Kontrolle über die Transaktionsaufreihung an eine Person delegieren, die den größten Kapitalpool kontrolliert.



Der Unterschied liegt in der Einsatzfähigkeit des Kapitals. PoW schließt Kapital aus, das nicht in Arbeit umgewandelt werden kann, während PoS Kapital ausschließt, das keine

Referenzen

[1] Kapitel: Proof-of-Memory-Fassade

[2] Kapitel: Fehlschluss der Energieverschwendung

[3] Kapitel: Eigenschaft der Zensurresistenz

Einheiten des Coins erwerben kann. Dieser Unterschied hat wesentliche Auswirkungen auf die Sicherheit.

Im Prinzip der anderen Mittel[1] wird gezeigt, dass Zensurresistenz davon abhängt, dass Menschen Miner dafür bezahlen, den Zensor zu überwältigen. **In einem PoS-System ist es nicht möglich, die Zensur zu überwinden, da der Zensor die Mehrheitsbeteiligung erworben hat und nicht abgesetzt werden kann.** Daher sind PoS-Systeme nicht zensurresistent und die Theorie ist demzufolge ungültig.

Referenzen

[1] Kapitel: Prinzip der anderen Mittel

Fehlschluss des Wiederholungsschutzes

Es gibt eine Theorie, dass Wiederholungsschutz[1], der in einer abgespaltenen Blockchain angewendet wird, den relativen Nutzen der ursprünglichen Blockchain erhöht. Wiederholungsschutz ist eine Regel, die relativ zu einer anderen Blockchain und mit gerichtetem Verhalten entwickelt wurde. Der Schutz macht Transaktionen der geschützten Blockchain auf der anderen ungültig.

Auch ohne Schutz ist es einem Eigentümer möglich, Ausgaben auf eine Weise zu tätigen, die eine Wiederholung in die eine oder andere Richtung verhindert, obwohl dies mit Gebühren und/oder Komplexitätskosten verbunden ist. Eine Aufteilung kann diese Kosten in eine oder beide Richtungen reduzieren, aber nicht eliminieren, indem Regeln aktiviert werden, die Ausgaben selektiv nutzen können. Dies wird als Opt-In bezeichnet, im Gegensatz zum obligatorischen Wiederholungsschutz. Opt-In-Wiederholungsschutz reduziert die Kosten, eliminiert sie aber nicht, während obligatorischer Schutz die Kosten eliminieren kann.

Die Wiederholung einer Ausgabe auf einer anderen Blockchain ist nicht verwässernd[2]. Die gemeinsame Ausgabe kann auf jeder Blockchain mit oder ohne Wiederholung ausgegeben werden. **Der einzige Unterschied, der durch den Schutz entsteht, besteht darin, dass die Ausgaben auf jeder Blockchain immer unterschiedlich sein können, ohne dass zusätzliche Kosten für den Ausgebenden entstehen.** Das Angebot in jeder Blockchain bleibt vom Schutz unberührt.

Es ist ein merkwürdiger Irrtum, dass eine Blockchain bei einer Aufspaltung irgendwie die Transaktionen einer anderen absorbieren kann. Alle Ausgaben des gemeinsamen

Referenzen

[1] https://de.wikipedia.org/wiki/Replay-Angriff

[2] https://de.wikipedia.org/wiki/Kapitalverwässerung

Segments bleiben auf beiden Blockchains auszahlbar. Der Wiederholungsschutz reduziert lediglich die Kosten für die Ausgabe auf der geschützten Blockchain.

Man könnte annehmen, dass der fehlende Schutz einen Besitzer weniger dazu veranlasst, Ausgaben auf der ungeschützten Blockchain zu tätigen, wodurch das Angebot begrenzt und der Umtauschpreis erhöht wird. Dies setzt jedoch voraus, dass die Nachfrage durch Erhöhung der Kosten für den Handel nicht beeinflusst wird. Wenn der Besitzer aufgrund der damit verbundenen erhöhten Kosten nicht handelt, wird der Nutzen des Coins nicht erhöht, sondern verringert.

Die Kosten des Selbstschutzes belaufen sich auf eine einmalige Demurrage[1], die so lange anhält, bis ungeschützte Einheiten absichtlich oder unabsichtlich geschützt werden. Diese Kosten stellen einen Abschlag[2] auf den Nutzen einer ungeschützten Blockchain im Vergleich zu einer hypothetischen gleichen Blockchain mit Schutz dar. Dies impliziert einen *größeren* Nutzen einer geschützten Blockchain im Vergleich zu der ungeschützten Blockchain, von der sie getrennt wird, als dies sonst der Fall wäre. Daher ist die Theorie ungültig.

Referenzen

[1] https://de.wikipedia.org/wiki/Demurrage_(Seefahrt)

[2] https://de.wikipedia.org/wiki/Kapitalwert

Definition von Shitcoin

Ein Shitcoin ist jedes System, das nicht kryptodynamisch sicher[1] ist, aber dennoch behauptet, das Wertversprechen[2] von Bitcoin zu haben.

Shitcoins gelten als Betrug, obwohl es möglich ist, dass ihre Befürworter zwar gute Absichten haben, aber dennoch ignorant gegenüber kryptodynamischen Prinzipien sind. Proof-of-Stake[3]-Technologien sind beispielsweise Shitcoins.

Auch wenn es möglicherweise Implementierungen von Bitcoin gibt, die sicherer sind als andere, ist dies eine Frage der Abstufungen. Es kann nicht nachgewiesen werden, dass ein Bitcoin absolut sicher[4] ist. Daher ist der Begriff auf keinen Bitcoin sinnvoll anwendbar. Beispielsweise sind Proof-of-Memory[5]-Technologien möglicherweise keine Shitcoins (auch wenn sie zentrale Zielsetzungen nicht erfüllen).

Referenzen

[1] Kapitel: Kryptodynamische Prinzipien

[2] Kapitel: Wertversprechen

[3] Kapitel: Proof-of-Stake-Fehlschluss

[4] Kapitel: Widerstandsaxiom

[5] Kapitel: Proof-of-Memory-Fassade

Fehlschluss der geteilten Kreditausweitung

Es gibt eine Theorie, dass die Erhöhung der Geldeinheiten, wie im Falle einer Teilung oder eines neuen Coins, Kredit erschafft. Dies ist ein Irrtum, der vermutlich eine Folge der Annahme ist, dass die durch staatliche Geldausweitung getriebene Kreditausweitung[1] eine Kraft des Marktes ist. Diese Annahme berücksichtigt nicht, dass Marktgeld[2] keine Seigniorage[3] erzeugen kann.

Seigniorage ist eine Steuer. Die geschaffenen Geldeinheiten stellen kein neues Kapital dar, sondern die Verwässerung bestehender Einheiten durch den Staat, wodurch das Eigentum an dem Kapital, das sie repräsentieren, auf den Souverän übertragen wird. Da dieses Kapital zur Subventionierung von Krediten durch das Staatsbanken[4]-Kartell in Form von diskontiertem Geld[5] und Versicherungen[6] eingesetzt wird, sinken die Kapitalkosten für die Kunden der Bank.

Diese sogenannte Kreditausweitung ist nicht einfach das Ergebnis des Teilreserve-Bankwesens als Marktmacht, sondern die Folge der Bevorzugung der Schuldner durch den Staat auf Kosten der Sparer. In einem freien Bankenmarkt sind Banken einfach *Investmentfonds*. Anleger erhalten im Durchschnitt eine marktübliche Kapitalrendite und tragen das damit verbundene Risiko. Im staatlichen Bankenwesen werden Risiken und damit auch Kapital nach politischen Zielen umverteilt.

Referenzen

[1] Kapitel: Fehlschluss der Kreditausweitung
[2] Kapitel: Taxonomie des Geldes
[3] https://de.wikipedia.org/wiki/Seigniorage
[4] Kapitel: Staatsbankenprinzip
[5] https://www.frbdiscountwindow.org
[6] https://www.fdic.gov/resources/deposit-insurance

Die Kreditausweitung des Marktes ist eine Erhöhung der Kapitalvergabe im Gegensatz zu dessen Hortung. Erhöhte Kreditzinsen sind eine Folge verringerter Zeitpräferenz[1] und senken die Kapitalkosten. Es ist unmöglich zu beweisen, dass die Schaffung eines neuen Coins (oder irgendetwas anderem) die Zeitpräferenz verringert. Daher ist es ein Fehler anzunehmen, dass diese Kreationen entweder die Verfügbarkeit von Kapital erhöhen oder dessen Kosten senken.

Referenzen

[1] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

Dilemma der Split-Spekulation

Im Zuge einer Aufspaltung steht der ursprüngliche Besitzer des Coins vor der Wahl, Einheiten der ursprünglichen und der geteilten Blockchain zu behalten oder zu verkaufen.

Wie im Dumping-Fehlschluss[1] erläutert, gibt es keine Möglichkeit, die Existenz der einen oder anderen Blockchain durch Austausch oder Hortung[2] von Einheiten der einen oder anderen zu verhindern. Daher betrachten wir diese Wahl ausschließlich als eine Frage der Maximierung des Wertes bestehender Bestände nach einer Aufspaltung.

Wenn der Split bevorsteht, dann ist ein Eigentümer von den steigenden Kosten der Umrechnung und gegebenenfalls des Wiederholungsschutzes[3] betroffen. Das sind unvermeidbare zukünftige Handelskosten, welche den Kapitalwert[4] der Einheiten mindern. Daher sind diese Faktoren für die Frage nicht relevant.

Die restlichen Überlegungen *gehen davon aus*, dass die kombinierten Coins im vorgesehenen Zeitraum im Preis steigen werden.

Unter den Annahmen des Konsolidierungsprinzips[5] werden sich zwei ähnliche Coins schließlich konsolidieren, wodurch der Wert eines von ihnen im Laufe der Zeit auf null sinkt. Wenn man zufällig weiß, welcher dies sein wird, ist es vernünftig, ihn zu verkaufen und den anderen zu kaufen. Da man jedoch möglicherweise *nicht* weiß, welcher Coin überleben wird, besteht die Möglichkeit, dass beim Handel der erfolgreiche Coin für den erfolglosen verkauft wird, wodurch der *gesamte* Wert der ursprünglichen

Referenzen

[1] Kapitel: Dumping-Fehlschluss
[2] https://en.m.wikipedia.org/wiki/Hoarding_(economics)
[3] Kapitel: Fehlschluss des Wiederholungsschutzes
[4] https://de.wikipedia.org/wiki/Kapitalwert
[5] Kapitel: Konsolidierungsprinzip

Einheiten verloren geht. **Ohne Wissen über die Zukunft erhöht der Verkauf des einen oder eines Teils davon für den anderen den potenziellen Gewinn im Verhältnis zum erhöhten Risiko.** Daher ist es ebenso vernünftig, beide zu horten, wodurch die Annahmen gewahrt werden, die vor der Aufspaltung bestanden.

Abschließend sollte betont werden, dass beide Blockchains scheitern könnten, wobei sich der Wert zu einer unabhängigen Blockchain, Ware oder *Staatsgeld* konsolidieren würde. Dieses Thema soll lediglich einen rationalen Entscheidungsrahmen basierend auf Annahmen bieten, die möglicherweise nicht eintreffen.

WIRTSCHAFT

Fehlschluss der Kreditausweitung

Kreditausweitung ist die Vervielfachung des Kredits gegenüber dem Geld[1], welche durch Kreditvergabe entsteht. Wenn ein Kredit vergeben wird, scheinen Kreditgeber und Kreditnehmer dasselbe Geld zu besitzen. Aufgrund der offensichtlich inflationären[2] Natur der Kreditexpansion wird sie im Allgemeinen als negative Auswirkung auf die Menschen angesehen, die das Geld halten. Da Banken die sichtbarsten Kreditgeber sind, wird dieser Effekt oft dem Bankwesen selbst zugeschrieben. Es gibt eine Theorie, dass Bitcoin die Auswirkungen des Teilreservebankwesens[3] beseitigen und dadurch die Kreditausweitung verhindern kann.

Sparen umfasst Horten und Investieren. Horten bedeutet laufende Wertminderung[4], was tatsächlich Konsum ist. Investieren ist Kreditvergabe zur Produktion und bedeutet keine Wertminderung, da Produkte erst existieren müssen, bevor sie an Wert verlieren können. Investieren umfasst sowohl Schuld- als auch Eigenkapitalverträge, da die Unterscheidung rein finanzieller Natur ist und keine wirtschaftliche Bedeutung[5] hat.

Referenzen

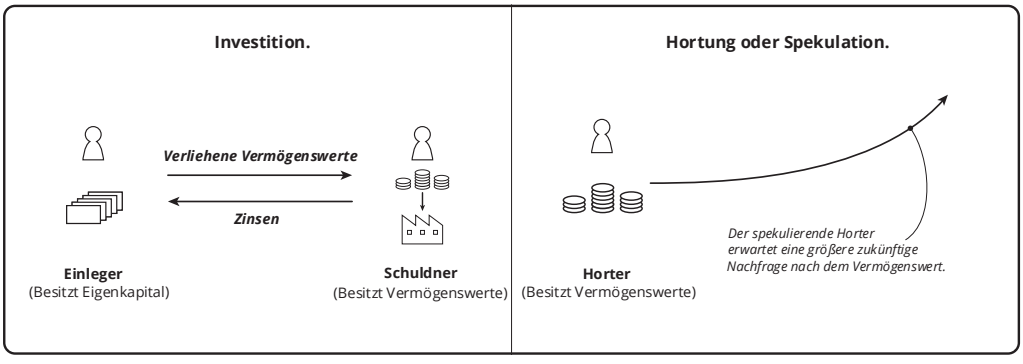
[1] Kapitel: Taxonomie des Geldes

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] https://de.wikipedia.org/wiki/Mindestreserve-System

[4] Kapitel: Abschreibungsprinzip

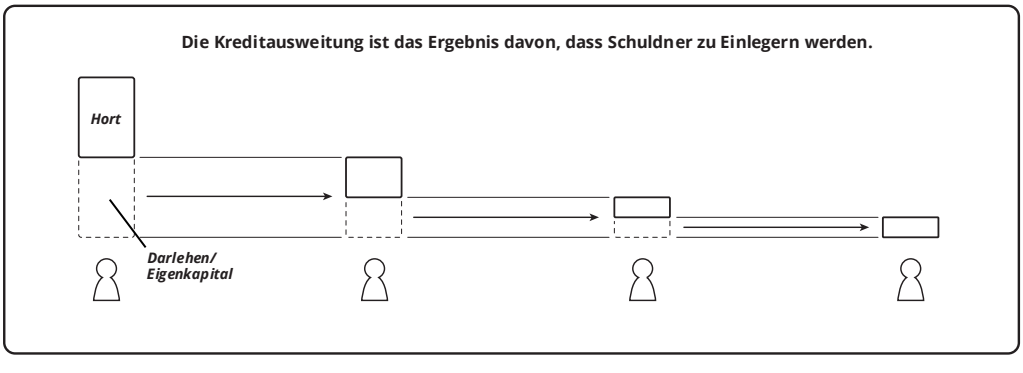
[5] https://mises.org/online-book/man-economy-and-state-power-and-market/5-marginal-utility-money/consumer



Die Unterscheidung zwischen Horten und Investieren ist für das Verständnis der Kreditausweitung von wesentlicher Bedeutung. Gehortetes Geld steht unter der Kontrolle seines Besitzers, als ob es in einem Tresorraum, im Hinterhof vergraben oder in eine Matratze gestopft wäre.

Dies ist inhärent in der Bedeutung von Eigentum. Der Geldverleiher ist nicht der Eigentümer des Geldes, auch wenn ein Darlehen als Ersparnis gilt.

Ein Kreditgeber benötigt Liquidität, um operieren zu können, und muss daher einen bestimmten Anteil seiner Ersparnisse horten. Wenn ein Kredit vergeben wird, gehört der geliehene Betrag dem Kreditnehmer. Der Kreditnehmer benötigt ebenfalls Liquidität und hortet daher einen bestimmten Anteil des Kredits. Der Rest des Kredits wird zwangsläufig investiert. Dies bedeutet, dass der Kreditnehmer zum Kreditgeber geworden ist. Dieser Prozess wird fortgesetzt, bis alles vorhandene Kapital gehortet ist.



Der gehortete Betrag wird manchmal als „Reserve“ des Eigentümers bezeichnet, aber korrekterweise ist es der Hort des Eigentümers, ein Bruchteil seiner gesamten Ersparnisse. Diese Verwendung des Wortes Reserve sollte nicht mit seiner Verwendung im Zusammenhang mit staatlichem Geld verwechselt werden, nämlich mit Reservewährung[1] (d.h. Devisenreserven[2]). Der Begriff „Teilreservebankwesen“ bezieht sich auf das Verhältnis des Horts einer Bank zu ihrem ausgegebenen Kredit (Geldkonten).

Die Gesamtmenge der im Umlauf befindlichen US-Dollars[3] wird als „M0“ bezeichnet. Dazu gehören alle materiellen Währungen („Bargeld in Tresoren“) sowie immaterielle Bankguthaben auf Konten der Federal Reserve. Diese beiden Formen gelten als austauschbare Verbindlichkeiten der Fed[4]. Bei den immateriellen Verbindlichkeiten handelt es sich um Geld, das verbucht, aber noch nicht gedruckt[5] ist. Wie von der Fed berichtet[6], beträgt die Gesamtsumme der US-Dollars:

Dollar	Betrag (2019)
Materiell	1.738.984.000.000 $
Immateriell	1.535.857.000.000 $
Gesamtgeldmenge (M0)	3.274.841.000.000 $

M0 plus sämtliches Bankguthaben wird als „M3“ bezeichnet. Dieses wird von der Fed nicht mehr veröffentlicht, wird aber auf 17.682.335.000.000 US-Dollar geschätzt[7]. Die Gesamtsumme der in US-Dollar gewährten Kredite kann aus der Summe der in Dollar

Referenzen

[1] Kapitel: Fehlschluss der Reservewährung

[2] https://de.wikipedia.org/wiki/Währungsreserve

[3] https://de.wikipedia.org/wiki/Geldmenge#Federal_Reserve_System

[4] https://de.wikipedia.org/wiki/Geldmenge

[5] Kapitel: Staatsbankenprinzip

[6] https://www.federalreserve.gov/releases/h3/current/default.htm

[7] https://fred.stlouisfed.org/series/MABMM301USM189S

denominierten Bankkonten[1], Anleihen[2], öffentlichen[3] und privaten Kapitalanlagen[4] geschätzt werden.

Dollar-Kredit	Betrag (2019)
Bank (M3-M0)	14.407.494.000.000 $
Anleihen	41.000.000.000.000 $
Öffentliche Kapitalanlagen	32.891.169.631.125 $
Private Kapitalanlagen	6.426.333.525.358 $

Aus der Tabelle:

- Das Gesamtverhältnis von Geld zu Kredit beträgt ~3,46 %, oder eine Kreditausweitung von 29,9 x Geldmenge.
- Bankreserven[5] von 1.400.949.000.000 US-Dollar deuten auf eine Bankreservequote von ~11,11 % gegenüber Bankkrediten oder auf eine Kreditausweitung von 9,0 x Geldmenge hin. Das liegt leicht über der erforderlichen Reservequote[6], die nicht mehr als 10 %[7] beträgt.
- Die Reserve des verbleibenden Geldes (d. h. ohne Bankreserven) im Verhältnis zu den Anleihen- und Aktienmärkten (d. h. das Verhältnis von M0 abzüglich Bankreserven zur Summe der Anleihen und des Eigenkapitals) beträgt ~2,08 %, oder eine Kreditausweitung von 48,0 x Geld.

Referenzen

[1] https://de.wikipedia.org/wiki/Bankkonto

[2] https://www.forbes.com/sites/kevinmcpartland/2018/10/11/understanding-us-bond-market/

[3] https://data.worldbank.org/indicator/cm.mkt.lcap.cd

[4] https://www.quora.com/What-is-the-estimated-total-value-of-all-US-private-companies

[5] https://www.federalreserve.gov/releases/h3/current/default.htm

[6] https://de.wikipedia.org/wiki/Mindestreserve

[7] https://en.wikipedia.org/wiki/Reserve_requirement#United_States

Die Beseitigung der Kreditausweitung erfordert die Beseitigung des Kredits und damit der Produktion. Bei allen Krediten kann es zu Zahlungsausfällen kommen. Es hält sich jedoch die Theorie, dass Bankkredite anders seien und sie so als "risikofrei" angenommen werden könnten. Diese Annahme erwächst aus der Tatsache der Steuerzahler-Versicherung[1] des Kredits. Dies ist keine Folge des Bankwesens, sondern der staatlichen Intervention in das Bankwesen. Soweit diese Annahme dem freien Bankwesen[2] zugeordnet wird, ist die Theorie ungültig. Alle Arten von Geschäften unterliegen dem Risiko des Scheiterns, und auf diese Weise beseitigt das freie Bankwesen diese Fehleinschätzung.

Die Unterscheidung zwischen einem Geldmarktfonds[3] (Money Market Fund, MMF) und einem Tagesgeldkonto[4] (Money Market Account, MMA) ist aufschlussreich. Beide sollen eine Eins-zu-eins-Äquivalenz mit Geld aufrechterhalten, doch beide sind aufgrund von Abwicklungs-[5] und Risikokosten gegenüber Geld diskontiert (z.B. akzeptieren manche Leute nur Bargeld und lehnen die höheren Kosten von Kreditkarten[6] und Schecktransaktionen[7] ab). Der Unterschied (abgesehen von der Steuerzahlerversicherung des letzteren) liegt in der Behandlung des Anlagerisikos und der unzureichenden Reserve.

Bei einem Geldmarktfonds schlägt sich ein Anlageversagen im Anteilspreis nieder. Während der Fonds versucht, einen ausreichenden Nettoinventarwert[8] (Net Asset Value, NAV) aufrechtzuerhalten, um den Tausch einer Einheit des Fonds gegen eine

Referenzen

[1] https://www.fdic.gov
[2] https://de.wikipedia.org/wiki/Free_Banking
[3] https://de.wikipedia.org/wiki/Geldmarktfonds
[4] https://de.wikipedia.org/wiki/Tagesgeldkonto
[5] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)
[6] https://de.wikipedia.org/wiki/Kreditkarte
[7] https://de.wikipedia.org/wiki/Scheck
[8] https://de.wikipedia.org/wiki/Substanzwert

Einheit des Geldes zu ermöglichen, wird sich ein hinreichender Rückgang des Nettoinventarwertes im Anteilspreis niederschlagen. Im Falle eines Tagesgeldkontos werden solche Verluste durch Geldreserven aufgefangen. Wenn die Reserven nicht ausreichen, entweder aufgrund unerwarteter Abhebungen oder aufgrund von Anlageverlusten, scheitert das Tagesgeldkonto. Das Scheitern eines Tagesgeldkontos äußert sich in einem Bankansturm[1], bei dem einige Leute ihr Geld zurückbekommen und andere nicht. Ein unzureichender Nettoinventarwert eines Geldmarktfonds äußert sich in einem gleichmäßigen Rückgang des Anteilspreises.

Der Vorteil eines Tagesgeldkontos ist der, dass seine Einheiten fungibler[2] sind, obwohl sie immer noch gegen Geld diskontiert werden. Der Vorteil eines Geldmarktfonds besteht darin, dass die Verluste gleichmäßig verteilt sind. Es ist daher nicht überraschend, dass Tagesgeldkonten in der Regel vom Steuerzahler versichert, vom Staat strenger reguliert und als Bankkredite ausgewiesen werden. Es kommt selten vor, dass ein Geldmarktfonds "die Dollar-Parität verliert"[3], aber natürlich kann es passieren und passiert auch. Bankenpleiten kommen auch vor, werden aber durch die Versicherung des Steuerzahlers verschleiert.

Bankkredite sind nicht fungibel. Das zeigt sich im alltäglichen Gebrauch von Kreditkarten und Schecks. Beide sind mit einem erheblichen Risiko der Nichtabwicklung verbunden. Während dieses Risiko im Allgemeinen dem Kontoinhaber zugeschrieben wird (z. B. im Fall eines Tagesgeldkontos), ist es nicht von der Person zu unterscheiden, die den Kredit annimmt. Man könnte sich daher vorstellen, dass die Akzeptanz von Kreditkarten und Schecks gegen Geldmarktfonds ähnlich gehandhabt wird. Der Kredit würde als Geldäquivalent zirkulieren und das Risiko würde gleichmäßiger auf diejenigen verteilt, die von der Rendite seiner Anlage profitieren. Das freie Bankwesen hat die Möglichkeit, beide Modelle in dem von den Menschen gewünschten Ausmaß zu

Referenzen

[1] https://de.wikipedia.org/wiki/Bankansturm

[2] https://de.wikipedia.org/wiki/Fungibilität

[3] https://www.investopedia.com/articles/mutualfund/08/money-market-break-buck.asp

übernehmen, aber in jedem Fall wird der Kredit gegen Geld ausgeweitet, es wird Risiken und Geldersatzmittel[1] geben.

Die Entscheidung, ob man hortet oder investiert[2], hängt ausschließlich von der Zeitpräferenz[3] der jeweiligen Person ab. Die Zeitpräferenz kann nicht aus irgendwelchen Umständen abgeleitet werden. Sie ist, wie der Name schon sagt, eine menschliche Präferenz. Menschliche Präferenzen ändern sich und daher auch die Zeitpräferenz. Die Zeitpräferenz bestimmt den ökonomischen Zinssatz, der auch als Kapitalkosten betrachtet werden kann. Ein Anstieg der Kapitalkosten infolge einer steigenden Zeitpräferenz führt zu einer Verknappung des verfügbaren Kredits, ein Rückgang hat den gegenteiligen Effekt. Bei einer unendlichen Zeitpräferenz würde alles Kapital für den Konsum gehortet, was die gesamte Produktion beenden würde.

Es spielt keine Rolle, ob ein Kreditgeber als „Bank" bezeichnet wird, alle Investitionen implizieren dasselbe Verhalten. Wenn Banken mit einem 100-prozentigen Hort operieren würden, wären sie keine Kreditgeber. Dies bedeutet keine Verringerung der Kreditvergabe, da die Kreditvergaberate[4] allein durch die Zeitpräferenz bestimmt wird. Bitcoin kann verliehen werden und tut nichts, um die Kreditausweitung einzuschränken. Die Theorie ist daher ungültig.

Die Einstellung der Kreditausweitung ist gleichbedeutend mit dem Zustand unendlicher Zeitpräferenz, unendlichem Zinssatz, keinem für die Produktion verfügbaren Kapital und keinen für den Konsum verfügbaren Produkten. In Staaten, in denen Kredite

Referenzen

[1] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[2] Kapitel: Sparverhältnis

[3] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)

[4] Kapitel: Fehlschluss des unverleihbaren Geldes

gesetzlich beschränkt oder verboten sind (Wuchergesetze[1]), gehen Investitionen in Eigenkapitalinstrumente, an Kredithaie[2], oder die Produktion endet.

Referenzen

[1] https://de.wikipedia.org/wiki/Zinswucher

[2] https://de.wikipedia.org/wiki/Kredithai

Abschreibungsprinzip

Der Besitz eines Produkts geht vom Produzenten auf den Konsumenten (oder Produzenten) über, doch zu diesem Zeitpunkt findet weder Produktion noch Konsum[1] statt. Der Produzent hortet das Produkt vor dem Handel und der Konsument hortet es danach. Das Produkt existiert und wird schließlich zwischen Menschen gehandelt. Die Begriffe „Produzent“ und „Konsument“ sind Namen für die *Ziele* (Produktion und Freizeit) der beiden primären Wirtschaftsakteure. Der Produzent *beabsichtigt*, Kapital zu schaffen (aufzuwerten), während der Konsument beabsichtigt, es zu zerstören (abzuwerten). Ein Produzent, der nur besitzt, produziert nicht und ein Konsument, der nicht besitzt, konsumiert nicht. Aber der Hort (Bestand) des Produzenten mindert den Wert des Produkts genauso wie der des Konsumenten.

Der allgemeine Gebrauch des Begriffs „Konsum“ vermischt Zinsen und Wertminderung[2]. Die Tatsache eines Produktverkaufs stellt für den Investor Zinsen dar, nicht die Wertminderung des Produkts. Die Wertminderung eines Produkts ist *tatsächlicher* Konsum und stellt entweder die Inanspruchnahme eines Dienstes für seinen Eigentümer[3] (Nutzen) oder Verschwendung[4] dar. Verschwendung ist Wertminderung, der der Eigentümer keinen Wert beimisst. Nur Zerstörung spiegelt tatsächlichen Konsum wider, so wie nur Schöpfung tatsächliche Produktion widerspiegelt. Nur die *Handlung* ist ökonomisch bedeutungsvoll, der Name einer gegebenen Rolle ist es nicht. Der Nettoerlös eines Verkaufs vom Produzenten an den Konsumenten ist Zins, auch wenn er durch Reinvestition kapitalisiert wird.

Referenzen

[1] Kapitel: Produktion und Konsum

[2] https://de.wikipedia.org/wiki/Wertminderung

[3] https://mises.org/online-book/man-economy-and-state-power-and-market/4-prices-and-consumption/7-prices-durable-goods-and-their-services

[4] https://de.wikipedia.org/wiki/Abfall

Vermögen, definiert als angesammeltes Kapital, ist die Summe der Produkte. Alle Produkte werden immer gehortet und verlieren an Wert. Die Produktion schafft Produkte, wobei die Zinsen sowohl die Kosten als auch die Rendite der Produktion darstellen. Der Preis eines Produktes ist die Summe des Zinsgewinns auf die Investition und den Kosten aller Produkte, die zur Produktion konsumiert wurden. Jedes Produkt, das in eine neue Produktkomponente integriert wird, wird als unabhängiges Produkt vollständig abgeschrieben und kommt im neuen Produkt zur Geltung. Da die Summe der Produktionskosten dem Nominalbetrag[1] entspricht, handelt es sich beim Produktzuwachs lediglich um Zinsen.

Die Wachstumsrate des Vermögens ergibt sich aus der Differenz zwischen Zinssatz und Abschreibungsrate.

```
Wachstumsrate = Zinssatz - Abschreibungsrate
```

Die folgenden Beispiele veranschaulichen die Auswirkungen der Abschreibung auf das Wachstum:

```
Wachstumsrate = Zinssatz - Abschreibungsrate
5% = 10% - 5%
-10% = 10% - 20%
```

Die Abschreibungsrate ist immer positiv, da jeder Besitz an Wert verliert.

```
Abschreibungsrate > 0
Zinssatz - Wachstumsrate = Abschreibungsrate
Zinssatz - Wachstumsrate > 0
Zinssatz > Wachstumsrate
```

Referenzen

[1] https://en.wikipedia.org/wiki/Bond_(finance)#Principal

Jedes Eigentum unterliegt einem Wertverlust, was bedeutet, dass der wirtschaftliche Nutzen immer größer ist als das Wirtschaftswachstum.

Der ökonomische Zinssatz kann im Zeitverlauf als Rendite des investierten Kapitals beobachtet werden.[1]

> Anleger erwarten eine Rendite von 10,2 %, und die Millennials hoffen auf mehr.
>
> *Shroders: Globale Anlegerstudie*

Die Abschreibungsrate kann aus beobachteten Zins- und Kapitalwachstumsraten abgeleitet werden.[2]

> Das globale Wachstum im Jahr 2019 wurde auf 2,6 Prozent herabgestuft, [...] was auf einen schwächeren als erwarteten internationalen Handel und Investitionen zu Jahresbeginn zurückzuführen ist. Bis 2021 soll das Wachstum schrittweise auf 2,8 Prozent steigen.
>
> *Weltbank: Globale Wirtschaftsaussichten*

In diesem Fall wird einem Zinssatz von 10,2 % eine Abschreibung von 7,6 % gegenübergestellt, um ein Wachstum von 2,6 % zu erhalten.

```
Abschreibungsrate = Zinssatz - Wachstumsrate
10,2% - 2,6% = 7,6%
```

Referenzen

[1] https://www.schroders.com/en/insights/global-investor-study/investors-expect-returns-of-10.2-with-millennials-hoping-for-more

[2] https://www.worldbank.org/en/publication/global-economic-prospects

Dies steht im Einklang mit Schätzungen zur Kapitalabschreibung. Während Gebäude und Maschinen eine geringe Abschreibungsrate aufweisen, sind Fahrzeuge, Büroausstattung und Lebensmittelvorräte (zum Beispiel) viel höher.[1]

> Für den Zeitraum 1960-2000 liegen die drei Schätzungen für Maschinen und Ausrüstung bei 5,61 %, 5,42 % und 5,68 %. Für Gebäude liegen die Schätzungen bei 3,36 %, 3,43 % und 3,43 %.
>
> *OECD: Schätzung der Abschreibungsraten*

In dem Maße, in dem Geld[2] einen Gebrauchswert[3] aufweist, verliert es wie jedes andere Gut[4] an Wert. Fiatgeld wie Bitcoin oder der US-Dollar hat mutmaßlich keinen Gebrauchswert. Reines Geld weist aufgrund der Opportunitätskosten[5] entgangener Zinsen kein Wachstum auf. Mit anderen Worten, Zinsen sind die Erfassung des Zeitwerts, und Geldentwertung umfasst das Versäumnis, diesen Wert einzufangen.

```
Reingeldwachstumsrate = Zinssatz - Zinssatz
9% - 9% = 0%
```

Der tatsächliche Geldwert verringert sich außerdem durch Umlaufsicherungsgebühren[6].

```
Warengeldwachstumsrate = Reingeldwachstumsrate - Umlaufsicherungsrate
0% - 1% = -1%
```

Referenzen

[1] https://www.oecd.org/sdd/productivity-stats/35409605.pdf

[2] Kapitel: Taxonomie des Geldes

[3] https://de.wikipedia.org/wiki/Gebrauchswert

[4] https://de.wikipedia.org/wiki/Gut_(Wirtschaftswissenschaft)

[5] https://de.wikipedia.org/wiki/Opportunitätskosten

[6] https://de.wikipedia.org/wiki/Umlaufgesichertes_Geld

Die Wachstumsraten von inflationärem[1] und deflationärem Geld werden im Fehlschluss des unverleihbaren Geldes[2] dargestellt.

Referenzen

[1] https://en.wikipedia.org/wiki/Monetary_inflation

[2] Kapitel: Fehlschluss des unverleihbaren Geldes

Ausdrucksprinzip

Menschliche Handlungen sollten nicht mit Gütern verwechselt werden. Das Versäumnis, auf der grundlegendsten Ebene zwischen beiden zu unterscheiden, führt zu Fehlern mit erheblichen Folgen[1]. Handlungen sind im Grunde menschliche Vorlieben, die durch Güter zum Ausdruck gebracht werden, die die Objekte dieses Ausdrucks sind. Ohne Ausdruck ist eine Präferenz bloß ein Gedanke und ein Gut bietet keinen Dienst. Die Katallaktik[2] beschäftigt sich mit zum Ausdruck gebrachten Vorlieben, insbesondere Produktion[3], Handel, und Konsum[4].

Der menschliche Geist ist der Akteur (Person). Er hat Vorlieben, die er ausdrückt, indem er den Körper motiviert, über den er Kontrolle hat (besitzt). Dieser Körper ist sein Eigentum, ein Gut. Wenn sein Körper vollständig entwertet (tot) ist, hört der Geist auf, ein Akteur zu sein. Es ist nicht notwendig, körperlose Geister zu betrachten, da keine Handlung impliziert ist.

Die Katallaktik beschäftigt sich nicht mit rechtlichen, theologischen oder ethischen Konzepten der Menschheit. Der Turing-Test[5] ist ein ausreichendes Kriterium für die Definition der Menschheit. Die katallaktische Unterscheidung liegt in der Bildung von Präferenzen, unabhängig von jedem anderen Akteur. Eine Person ist in diesem Sinne ein Entscheidungs-Macher, im Gegensatz zu einem Regeln-Befolger. Eine Maschine ist ein Gut, das die Präferenzen einer Person zum Ausdruck bringt. Eine Person drückt ihre Präferenzen aus, indem sie ihre Maschine betreibt.

Referenzen

[1] https://de.wikipedia.org/wiki/Arbeitswerttheorie
[2] https://de.wikipedia.org/wiki/Katallaktik
[3] Kapitel: Produktion und Konsum
[4] Kapitel: Abschreibungsprinzip
[5] https://de.wikipedia.org/wiki/Turing-Test

Ein Geist kann kein Eigentum sein, und ein Körper ist das Eigentum seines Geistes. Nur der Geist kontrolliert den Körper, wobei Kontrolle Eigentum definiert. Wo der Geist durch die Aggression[1] eines anderen Akteurs zum Handeln gezwungen wird, ist die Präferenz nicht unabhängig. Die zum Ausdruck gebrachte Präferenz (Handlung) ist die des Aggressors.

Die Katallaktik berücksichtigt nur die Folgen unabhängiger Akteure. Wenn jemand bestohlen wird, drückt dies die Präferenz des Diebes aus, nicht seine eigene. Wenn jemand eine Steuer zahlt, wird davon ausgegangen, dass er die Präferenz einer anderen Person ausdrückt, da Steuern von Natur aus unfreiwillig sind. Sklaverei impliziert den Ausdruck der Präferenzen des Sklavenhalters, nicht die des Sklaven. Die Ersetzung der eigenen Präferenz durch die einer anderen Person ist unfreiwilliger Handel (Diebstahl).

Manchmal wird argumentiert, dass Zeit wertvoll ist, weil das Leben vergänglich ist. Dies ist jedoch nicht die Grundlage der Zeitpräferenz[2]. Die Unbeständigkeit einer Person ist für die Katallaktik ohne Bedeutung. Eine Person kann ewig leben und dennoch wird davon ausgegangen, dass sie ihre Präferenz zum Ausdruck bringt, Waren eher früher als später zu erhalten. Unendliches Leben bedeutet nicht, dass man kein Verlangen nach Konsum hat.

Eine Handlung ist der Ausdruck menschlicher Vorlieben durch Güter. Von Menschen gesteuerte Prozesse sind Handlungen, von Maschinen gesteuerte Prozesse sind Güter. Mit anderen Worten, Produktion/Arbeit[3], Handel/Diebstahl und Freizeit/Verschwendung sind Handlungen, während Websites, Fließbänder und Autos Güter sind.

Referenzen

[1] https://de.wikipedia.org/wiki/Nichtaggressionsprinzip

[2] Kapitel: Zeitpräferenzfehlschluss

[3] Kapitel: Arbeit und Freizeit

Vollreservefehlschluss

Es gibt eine Theorie, dass das Teilreserve-Bankwesen[1] ein Betrug ist, der es den Banken ermöglicht, Geld[2] „aus dem Nichts"[3] zu erschaffen. Diese Theorie impliziert, dass ehrliches Bankwesen auf Vollreserve[4] basieren muss

Diese Theorie hängt von der Definition des Wortes „Bank" ab. Rothbard[5] führt das obige Argument in Mensch, Wirtschaft und Staat an, beschränkt seine Definition einer Bank[6] jedoch ausdrücklich auf die eines „Lagers" für Geld:

> Wenn jemand Waren in einem Lagerhaus deponiert, erhält er einen Beleg und zahlt dem Eigentümer des Lagerhauses einen bestimmten Betrag für die Lagerung. Er behält weiterhin das Eigentum an der Ware; der Eigentümer des Lagerhauses bewacht sie lediglich für ihn. Bei Vorlage des Lagerscheins ist der Eigentümer verpflichtet, die deponierte Ware herauszugeben. Ein auf Geld spezialisiertes Lagerhaus wird als „Bank" bezeichnet.
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Banken bieten diesen Lagerservice im Namen der sicheren Einlage[7] an. Aber Banken sind nicht so eng definiert. Sie bieten im Allgemeinen auch verzinsliche Konten wie Spareinlagen[8] und Termineinlagen[9] an. Rothbard verwendet die Erwartung von Zinsen um die Lagerung von Geld von der Kreditvergabe zu unterscheiden:

Referenzen

[1] https://de.wikipedia.org/wiki/Mindestreserve-System

[2] Kapitel: Taxonomie des Geldes

[3] Kapitel: Aus-dem-Nichts-Fehlschluss

[4] https://de.wikipedia.org/wiki/Vollreserve-System

[5] https://de.wikipedia.org/wiki/Murray_Rothbard

[6] https://mises.org/online-book/man-economy-and-state-power-and-market/6-supply-money/b-claims-money-money-warehouse

[7] https://de.wikipedia.org/wiki/Schließfach

[8] https://de.wikipedia.org/wiki/Spareinlage

[9] https://de.wikipedia.org/wiki/Termingeld

Das Eigentum einer anderen Person wird vom Lagerhaus übernommen und für eigene Zwecke zur Geldbeschaffung verwendet. Es handelt sich dabei nicht um ein geliehenes Geld, da für die Nutzung des Geldes keine Zinsen gezahlt werden.

Mit anderen Worten, seine Forderung nach einer Vollreserve gilt nicht für verzinsliche Konten. Allerdings versäumt er es, darauf hinzuweisen, dass die Zinsen, die auf das durch Einlagen repräsentierte Geld verdient werden, legitimerweise die sonst notwendigen Kontogebühren ausgleichen können.

Banken bieten häufig zinslose Sichtkonten[1] (z.B. Girokonten) an. Die Tatsache, dass das Konto einen positiven Ertrag erwirtschaftet, ist nicht die Abgrenzung zwischen Lagerung und Kreditvergabe, nicht einmal nach seiner eigenen Definition. Wenn ein Bankkonto 5 % Ertrag bei einem Gebührensatz von 6 % bringt, gibt es keinen Unterschied zu 0 % Ertrag bei einem Gebührensatz von 1 %. Der Unterschied ist die vertragliche Vereinbarung zwischen dem Einleger und der Bank.

Da es bequemer ist, Papiergeld im Tausch zu übertragen, als Gold mitzuführen, werden Geldlager (oder Banken), die das Vertrauen der Öffentlichkeit stärken, feststellen, dass nur wenige Menschen ihre Zertifikate einlösen.

Geldzertifikate, die gelagertes Geld repräsentieren, sind repräsentatives Geld[2], eine Form des Geldersatzes[3]. In den Vereinigten Staaten wurden solche Zertifikate früher von

Referenzen

[1] https://de.wikipedia.org/wiki/Girokonto

[2] https://en.wikipedia.org/wiki/Representative_money

[3] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

Staatsbanken[1] und anderen Stellen ausgegeben. Diese wurden schließlich durch von der Zentralbank[2] ausgegebene Gold-[3] und Silberzertifikate[4] ersetzt.

> Die Banken werden besonders der Versuchung ausgesetzt sein, Betrug zu begehen und Pseudogeldzertifikate auszugeben, die neben echten Geldzertifikaten als akzeptabler Geldersatz in Umlauf gebracht werden. Da Geld ein homogenes Gut ist, ist es den Menschen gleichgültig, ob das Geld, das sie einlösen, das ursprüngliche Geld ist, das sie eingezahlt haben. Dies macht es den Banken leichter, Betrug zu begehen.

Sofern Zentralbankzertifikate jemals das gesamte gelagerte Geld repräsentierten (z. B. Gold und Silber), folgten sie letztendlich dem von Rothbard beschriebenen Verlauf.

Als die Summe der Zertifikate zu groß wurde, um sie einlösen zu können, wurden sie für ungültig erklärt und die Menschen waren gezwungen[5], sie in Fiatgeld umzutauschen. Diese groß angelegten Betrügereien fanden zu Lebzeiten sowohl von Rothbard als auch von seinem Vorgänger von Mises[6] statt und wurden von Staats- und Zentralbanken unter dem Schutz des Gesetzes (d. h. des Staates) begangen.

Die Theorie beschränkt ihre Verurteilung des Bankwesens nicht auf den Betrug bei der Einlagerung (bei Bankeinlagen), sondern erstreckt sich auch auf die ehrliche Kreditvergabe von Einlagen durch Banken im Allgemeinen, einschließlich Sichteinlagen, Spareinlagen und oft auch Termineinlagen. Daher ist die Theorie ungültig. Darüber hinaus impliziert sie eine Verurteilung des Verleihens und

Referenzen

[1] https://en.wikipedia.org/wiki/State_bank
[2] https://de.wikipedia.org/wiki/Zentralbank
[3] https://en.wikipedia.org/wiki/Gold_certificate
[4] https://en.wikipedia.org/wiki/Silver_certificate
[5] https://en.wikipedia.org/wiki/Gold_Reserve_Act
[6] https://de.wikipedia.org/wiki/Ludwig_von_Mises

Investierens im Allgemeinen. Und wie Rothbard selbst betont[1], ist das Verleihen nicht vom Investieren zu unterscheiden:

> Ob das angesparte Kapital in Form von Aktien oder Krediten investiert wird, ist unerheblich. Der einzige Unterschied liegt in den juristischen Details. Und selbst der rechtliche Unterschied zwischen Gläubiger und Eigentümer ist vernachlässigbar.

Alle Kredite stammen aus dem angesammelten Kapital einer Person, unabhängig davon, ob es bei einer Bank oder auf andere Weise hinterlegt ist. Es gibt keine andere Quelle für Kredite als angelegte Ersparnisse. Es gibt eine damit verbundene Theorie[2], dass die Leute zu dumm sind, um die vertraglichen Bedingungen einer Einlage zu verstehen.

> Huerta de Soto erwägt die Möglichkeit, „dass eine bestimmte Gruppe von Bankkunden (oder der Argumentation halber alle) einen Einlagenvertrag abschließt, in dem Bewusstsein und mit der vollen Akzeptanz, dass Banken einen großen Teil des von ihnen eingezahlten Geldes anlegen (oder verleihen usw.) werden". In diesem Fall, argumentiert Huerta de Soto, „fehlt der vermeintlichen Ermächtigung der Einleger die rechtliche Gültigkeit", weil nur wenige Laien die dem Teilreserve-Bankwesen innewohnende Instabilität verstehen: Sie glauben, ihre Einlage sei garantiert, was Huerta de Soto für ein (beinahe universelles) Missverständnis hält.
>
> *Wikipedia: Jesús Huerta de Soto*

Doch diejenigen, die dieses Argument vorbringen, glauben, es verstehen zu können. Daher ist die Theorie ungültig. Angesichts der moralischen Unterscheidung des Nichtaggressionsprinzips[3] hat jeder Mensch das Recht, freiwillig Verträge mit anderen abzuschließen. Dieses Recht zu entziehen wäre ein Verbrechen. Verweise auf „Banklose" setzen im Allgemeinen voraus, dass eine große Zahl von Menschen keinen „Zugang" zu Bankdienstleistungen hat. Dies ist im Allgemeinen nicht der Fall; Bankgeschäfte sind

Referenzen

[1] https://mises.org/online-book/man-economy-and-state-power-and-market/6-production-rate-interest-and-its-determination/9-joint-stock-companies-and-producers-loan-market

[2] https://en.wikipedia.org/wiki/Jesús_Huerta_de_Soto#Austrian_business_cycle_and_full_reserve_banking

[3] https://de.wikipedia.org/wiki/Nichtaggressionsprinzip

überall auf der Welt verfügbar. Es sind die Menschen, die die Risiken verstehen[1] und entscheiden, sie nicht einzugehen.

Eine verwandte Theorie besagt, dass Geldersatz zum gleichen Wert wie das Geld gehandelt wird, was Betrug darstellt. Sofern Geldersatz (z. B. Einlagenkonten) vom Steuerzahler versichert sind[2] ist der Abschlag gegenüber dem Geld, das sie ersetzen, geringer. Selbst bei vollständiger Versicherung ist es jedoch ein Fehler anzunehmen, dass diese zum Nennwert des Geldes gehandelt werden. Geldersatz tritt als Einlagenkonto auf und wird in der Regel elektronisch abgewickelt. Die Abrechnung[3] von Geldkonten ist mit Zeit-, Geld- und Risikokosten verbunden. Kreditkarten- und Scheckbetrug sind weit verbreitet[4] und diese Kosten schlagen sich in allen Transaktions- und Kontogebühren nieder. Die Abrechnung kann Tage[5], wenn nicht Monate[6] dauern. Händler diskontieren Geldersatzmittel[7] gegenüber Geld. Selbst elektronische Überweisungen zwischen Banken erzeugen erhebliche Abwicklungskosten[8]:

> Den Banken wird für jede Transaktion eine Bruttoüberweisungsgebühr von 0,82 US-Dollar berechnet. Es gibt jedoch einen dreistufigen Rabattplan, sodass die tatsächlichen Transaktionsgebühren je nach Transaktionsvolumen zwischen 0,034 und 0,82 US-Dollar pro Transaktion liegen.
>
> *Wikipedia: Fedwire*

Aus diesem Grund akzeptieren viele Geschäfte nur Bargeld, andere akzeptieren keine Schecks, andere verlangen einen Aufschlag, um die Abwertung auszugleichen, und es

Referenzen

[1] https://www.reuters.com/article/zimbabwe-crisis-cbank/zimbabwe-c-bank-says-raided-private-bank-accounts-idUSLK23553320090420

[2] https://www.fdic.gov/

[3] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)

[4] https://de.wikipedia.org/wiki/Kreditkartenbetrug

[5] https://en.wikipedia.org/wiki/Cheque_clearing

[6] https://en.wikipedia.org/wiki/Chargeback

[7] https://en.wikipedia.org/wiki/Merchant_account#Discount_rates

[8] https://en.wikipedia.org/wiki/Fedwire

gibt Geldautomaten-Entgelte[1], usw. Die Feststellung, dass Geldersatzmittel nicht diskontiert werden, wird also durch einen Berg von Gegenbeweisen widerlegt. Noch wichtiger ist, dass dieser Rabatt nachweislich notwendig ist, was die Theorie widerlegt.

Eine verwandte Theorie besagt, dass Bankkredite als Folge der Kreditausweitung[2] zu Preisinflation[3] führen. Da Kreditvergabe und Geld sich zwangsläufig gemeinsam entwickelt haben, gibt es nie einen Zeitpunkt, an dem die Kreditausweitung selbst den Grad des Geldersatzes verändert. Dies erfordert entweder eine Ausweitung der Geldmenge[4] oder eine Verringerung der Zeitpräferenz[5], die sich im wirtschaftlichen Zinssatz widerspiegelt. Die Kreditausweitung ist strenggenommen eine Funktion dieser beiden Faktoren, nicht der Kreditvergabe selbst. Daher ist die Theorie ungültig.

Eine verwandte Theorie besagt, dass Banken nur „ihr eigenes" Geld verleihen dürfen. Alles verliehene Kapital sind die Ersparnisse von jemandem. Wenn jeder eine Bank betreiben kann (d. h. auf seine eigenen Ersparnisse Kredite aufnehmen und diese an andere verleihen kann), dann ist dies ein Unterschied ohne Bedeutung. Die Zusammenlegung von Ersparnissen mit anderen Personen (d. h. durch Bankeinlagen) schafft keinen bedeutsamen Unterschied. Daher ist die Theorie ungültig.

Eine verwandte Theorie besagt, dass Banken Kredite nur gegen Termineinlagen vergeben dürfen. Es gibt keinen wirtschaftlichen Unterschied zwischen Termineinlagen und Sichteinlagen, da beide eine Teilreserve beinhalten. Die Art der Einlagen, selbst von Bankeinlagen, impliziert, dass für die Auszahlung Zeit und andere Einschränkungen (z.

Referenzen

[1] https://de.wikipedia.org/wiki/Geldautomaten-Entgelt

[2] Kapitel: Fehlschluss der Kreditausweitung

[3] https://de.wikipedia.org/wiki/Inflation

[4] https://de.wikipedia.org/wiki/Gold#Gewinnung

[5] Kapitel: Zeitpräferenzfehlschluss

B. Identifizierung) erforderlich sind. Sogar steuerzahlerversicherte Giro- und Sparkonten sind effektiv Termineinlagen[1]:

> Für alle Sparkonten und alle privaten verzinslichen Girokonten behalten wir uns das Recht vor, eine schriftliche Mitteilung über die Abhebung sieben Tage im Voraus zu verlangen.
>
> *Chase Bank: Einlagenvereinbarung*

Ausfallrisiko und Kreditausweitung bleiben trotz Fristenkongruenz bestehen. Daher ist die Theorie ungültig. Die einzige echte Sichteinlage ist überhaupt keine Einlage (Geld), und natürlich haben die Menschen diese Option und die der Termineinlage, sofern sie diese bevorzugen.

Eine verwandte Theorie besagt, dass Banken Kredite nur gegen voll versicherte Einlagen vergeben dürfen. Die einzige wirklich risikofreie Rendite[2] ist jedoch keine Rendite. Aus diesem Grund versichern nur Steuerzahler Kredite (d. h. durch Zwang). Eine vollständige Versicherung ist wirtschaftlich gleichbedeutend mit überhaupt keiner Kreditvergabe, was die Theorie zu einem Widerspruch und damit ungültig macht.

Eine verwandte Theorie besagt, dass sogar das freie Bankwesen[3] die Fähigkeit besitzt, Geld „aus dem Nichts"[4] zu erschaffen. Wenn das stimmt, kann das jedoch jeder, da das freie Bankwesen den Leuten, die sich selbst als Banken bezeichnen, keine besonderen Befugnisse verleiht. Wenn Geld kostenlos erschaffen werden kann, kann es kein Eigentum sein. Daher ist die Theorie ungültig. Sogar staatliches Geld verursacht Produktionskosten[5], Kosten für die Aufrechterhaltung seines Produktionsmonopols[6]

Referenzen

[1] https://www.chase.com/content/dam/chase-ux/documents/personal/checking/deposit-account-agreement.pdf

[2] Kapitel: Fehlschluss des risikofreien Zinssatzes

[3] https://de.wikipedia.org/wiki/Free_Banking

[4] Kapitel: Aus-dem-Nichts-Fehlschluss

[5] https://www.federalreserve.gov/faqs/currency_12771.htm

[6] https://en.wikipedia.org/wiki/Counterfeit

und politische Kosten[1] in Form der Geldinflation[2]. Aufgrund der Natur des Wettbewerbs genießt das freie Bankwesen, wie etwa bei Gold oder Bitcoin, kein Seigniorage[3]-Privileg.

Schließlich ist es häufig so, dass die Befürworter einer Vollreservekreditvergabe dieselben sind, die sich für niedrigere Zeitpräferenzen einsetzen. Dies ist ein direkter Widerspruch, da Ersteres eine unendliche Zeitpräferenz impliziert.

Referenzen

[1] https://en.wikipedia.org/wiki/Crisis_in_Venezuela

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] https://en.wikipedia.org/wiki/Seigniorage

Inflationsprinzip

Man nimmt an[1], dass sich die Kaufkraft[2] eines Geldes[3] proportional zur Nachfrage nach den Gütern ändert, die sie repräsentiert. Mit anderen Worten, bei der doppelten Geldmenge wird jede Einheit des Geldes für die Hälfte der vorherigen Warenmenge gehandelt, da die Zunahme an Waren eine geringere Nachfrage nach ihnen bedeutet. Dies ist eine proportionale Beziehung[4] zwischen Geldinflation[5] und Preisinflation[6] (oder Deflation). Diese Geldbeziehung[7] ist Ausdruck des Gesetzes von Angebot und Nachfrage[8].

- Ein steigendes Angebot an Marktgeld wie Gold und *frühem* Bitcoin verbraucht den gleichen Wert in Gütern, den es an neuen Einheiten schafft – einschließlich der Opportunitätskosten[9] des dafür investierten Kapitals. Daher führt es zu keiner Änderung der Proportionalität und daher auch zu keiner Preisinflation.
- Monopolgeld unterliegt keiner wettbewerblichen Produktion, sodass sein Produzent bei der Preisgestaltung neuer Einheiten eine Monopolprämie[10] erzielen kann. Dadurch erhöht sich das Verhältnis von Geld zu Gütern, was zu Preisinflation führt.

Referenzen

[1] https://mises.org/online-book/man-economy-and-state-power-and-market/11-money-and-its-purchasing-power/13-fallacy-equation-exchange

[2] https://de.wikipedia.org/wiki/Kaufkraft_(Konsum)

[3] Kapitel: Taxonomie des Geldes

[4] https://de.wikipedia.org/wiki/Proportionalität

[5] https://en.wikipedia.org/wiki/Monetary_inflation

[6] https://de.wikipedia.org/wiki/Inflation

[7] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/4-determination-purchasing-power-money

[8] https://de.wikipedia.org/wiki/Marktgleichgewicht

[9] https://de.wikipedia.org/wiki/Opportunitätskosten

[10] https://mises.org/online-book/man-economy-and-state-power-and-market/3-illusion-monopoly-price/definitions-monopoly

- Marktgeld mit festem Angebot, so wie späterer Bitcoin, schafft keine Einheiten. Daher sinkt das Verhältnis von Geld zu Gütern mit dem Wirtschaftswachstum, was zu einer Preisdeflation[1] führt.

Proportionalität bezieht sich auf die Güter, die durch ein Geld „repräsentiert" werden. Gäbe es nur ein Geld, wäre dies eine direkte Beziehung zu allen Gütern. Im Fall mehrerer Gelder muss diese Beziehung jedoch thematisiert werden. Die Güter, die durch ein Geld repräsentiert werden, sind jene, die gegen es eingetauscht werden können. Mit anderen Worten, die Beziehung impliziert eine Nachfrage nach Gütern in dem Geld.

Doch die Nachfrage bleibt nicht konstant, wenn man sich für das Mining entscheidet. Durch das Mining entsteht eine neue Nachfrage nach Gütern. Der Miner muss „repräsentative" Güter konsumieren, um das Geld zu produzieren. Das neue Geld wird vollständig durch die Nachfragesteigerung ausgeglichen, die durch die konsumierten Güter und die Opportunitätskosten (d. h. weniger neue Güter), die durch den Einsatz dieser Güter beim Abbau entstehen, repräsentiert wird. Daher bleibt die Proportionalität auch im Fall mehrerer Geldarten gewahrt. **In einem freien Markt ist Wirtschaftswachstum nicht preisinflationär.**

Indem er die kopernikanische[2] Quantitätstheorie[3] des Geldes erweiterte, formulierte Richard Cantillon[4] eine Theorie, die heute als Cantillon-Effekt[5] bekannt ist. Die Theorie ist gültig, wenn sie auf Monopolgeld angewendet wird, hat aber keine Relevanz für Marktgeld – eine Tatsache, die den Ökonomen seit Cantillon offenbar entgangen ist. Die Grundlage der von Cantillon erklärten Verzerrungen ist die Seigniorage[6], nicht die

Referenzen

[1] https://de.wikipedia.org/wiki/Deflation
[2] https://de.wikipedia.org/wiki/Nikolaus_Kopernikus
[3] https://de.wikipedia.org/wiki/Quantitätstheorie
[4] https://de.wikipedia.org/wiki/Richard_Cantillon
[5] https://de.wikipedia.org/wiki/Cantillon-Effekt
[6] https://de.wikipedia.org/wiki/Seigniorage

Geldproduktion. Die Marktproduktion von Geld ist, wie die Marktproduktion von allen Dingen, nicht nur neutral in realen Auswirkungen[1], sondern auch Preisneutral.

In *Menschliches Handeln*[2], versuchte Ludwig von Mises[3], wie seine Vorgänger, die Gültigkeit des Cantillon-Effekts für *jedes* Geld nachzuweisen[4].

> Änderungen in der Geldmenge müssen zwangsläufig die Verteilung der käuflichen Güter im Besitz verschiedener Einzelpersonen und Unternehmen verändern. Die im gesamten Marktsystem verfügbare Geldmenge kann nur durch eine Erhöhung oder Verringerung der Bargeldbestände bestimmter einzelner Teilnehmer erhöht oder verringert werden.
>
> *Ludwig von Mises: Menschliches Handeln*

Diese Aussage besagt, dass neues Geld zuerst bestehende Geldbestände beeinflusst. Dies ist jedoch bei Marktgeld nicht der Fall. Seine Schaffung *verringert die Warenbestände*, während es gleichzeitig die *Geldbestände erhöht*. Die erhöhte Nachfrage nach Geld wird gleichzeitig und proportional durch das erhöhte Angebot ausgeglichen. Dieser Verbrauch der Waren kann bei der Bewertung der Geldbeziehung nicht ignoriert werden. Die Aussage verwechselt Marktgeld mit Monopolgeld, da letzteres seinen Wert nicht bei dessen Produktion in Form von Waren verbraucht. Insofern die Güter im Wesentlichen am selben Ort und zur selben Zeit konsumiert werden, zu der auch das Geld produziert wird, ist noch nicht einmal eine ungleiche Verteilung der Geldverhältnisse impliziert. Dieser Fehler hält sich hartnäckig, obwohl ausdrücklich anerkannt wird, dass der Bergbau (Mining) den Wert in Gütern verbraucht, den er in Form von neuem Geld produziert.

Referenzen

[1] https://de.wikipedia.org/wiki/Neutralität_des_Geldes

[2] https://mises.org/online-book/human-action

[3] https://de.wikipedia.org/wiki/Ludwig_von_Mises

[4] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/4-determination-purchasing-power-money

> Die Tatsache, dass die Goldminenbesitzer auf stetige jährliche Einnahmen aus ihrer Goldproduktion angewiesen sind, hebt den Einfluss des neu geförderten Goldes auf die Preise nicht auf. Die Minenbesitzer beziehen vom Markt im Austausch für das geförderte Gold die Waren und Dienstleistungen, die sie für ihren Abbau benötigen [...]. Hätten sie diese Menge Gold nicht gefördert, hätte dies keinen Einfluss auf die Preise gehabt.

Wörtlich genommen ist der letzte Satz eine Tautologie[1] (keine Schöpfung impliziert keinen Preiseffekt durch die Schöpfung). Aus dem Kontext geht klar hervor, dass Mises meint, dass die Preise unverändert geblieben wären, wenn das Gold nicht produziert worden wäre. Doch ohne eine Änderung der Geldmenge wären die Güter in einem anderen Produktionsprozess[2] verbraucht worden und das implizite Wirtschaftswachstum hätte die Preise gesenkt, und wenn die Güter für die Freizeit[3] konsumiert würden, würde die implizite Wirtschaftskontraktion die Preise *erhöhen*. Mit anderen Worten, die obige Schlussfolgerung ist genau umgekehrt. Die Geldbeziehung bleibt aufgrund der Geldproduktion *erhalten* und würde sich aufgrund des Fehlens derselben ändern. Dieser Fehler infiziert dann abhängige Theorien.

> Gegen diese Argumentation muss man zunächst einmal feststellen, dass in einer fortschreitenden Wirtschaft, in der die Bevölkerungszahlen steigen und die Arbeitsteilung und ihre Folge, die industrielle Spezialisierung, perfektioniert werden, eine Tendenz zur Steigerung der Nachfrage nach Geld besteht. Es treten mehr Menschen auf den Plan, die Bargeld halten wollen. Der Grad der wirtschaftlichen Selbstversorgung, d. h. der Produktion für den Eigenbedarf der Haushalte, schrumpft und die Menschen werden abhängiger vom Markt; dies wird sie im Großen und Ganzen dazu zwingen, ihre Bargeldbestände zu erhöhen.

Mit anderen Worten, allein das Wirtschaftswachstum verändert die Geldbeziehung – ein direkter Widerspruch zur vorhergehenden Aussage.

Referenzen

[1] https://de.wikipedia.org/wiki/Tautologie_(Logik)

[2] Kapitel: Produktion und Konsum

[3] Kapitel: Arbeit und Freizeit

So steht der Preissteigerungstendenz, die von der sogenannten „normalen“ Goldproduktion ausgeht, eine Preissenkungstendenz gegenüber, die von der erhöhten Nachfrage nach Bargeldhaltung ausgeht. Diese beiden entgegengesetzten Tendenzen heben sich jedoch nicht gegenseitig auf. Beide Prozesse nehmen ihren eigenen Verlauf, beide führen zu einer Störung der bestehenden sozialen Bedingungen, wodurch einige Menschen reicher, andere ärmer werden. Beide beeinflussen die Preise verschiedener Waren zu unterschiedlichen Zeitpunkten und in unterschiedlichem Ausmaß. Es ist wahr, dass der durch einen dieser Prozesse verursachte Preisanstieg einiger Waren schließlich durch den durch den anderen Prozess verursachten Preisrückgang kompensiert werden kann. Es kann vorkommen, dass am Ende einige oder viele Preise auf ihren vorherigen Stand zurückkehren. Aber dieses Endergebnis ist nicht das Ergebnis fehlender Bewegungen, die durch Änderungen der Geldrelationen hervorgerufen wurden. Es ist vielmehr das Ergebnis der gemeinsamen Wirkung des Zusammentreffens zweier voneinander unabhängiger Prozesse.

Dies ist eine Widerlegung der Vorstellung, Geldschöpfung sei ein „Stimulus“[1] für Wachstum, was richtig ist. Doch wird fälschlicherweise angenommen, dass Geldnachfrage und Geldschöpfung voneinander unabhängige Prozesse sind. Sie sind ausdrücklich voneinander abhängig, wie es in der Geldbeziehung und dem Gesetz von Angebot und Nachfrage zum Ausdruck kommt, welches sie widerspiegelt. Die Wirkung unabhängiger Interaktionen wird in diesem Argument vollkommen umgekehrt, da sie die Geldbeziehung nur verschleiern kann. Stimulus ist eine Umkehrung von Ursache und Wirkung, die richtig widerlegt wurde, aber es ist ein Fehler, die Geldbeziehung sowohl zu akzeptieren als auch abzulehnen.

Der zugrundeliegende Inflationsfehlschluss kann, wie der des Regressionstheorems[2], aus einem verständlichen Wunsch resultieren, die nachteiligen Effekte[3] des Monopolgeldes zu erklären. Doch im rein rationalen System der Katallaktik[4] führt jeder Fehler in der Deduktion zu Inkonsistenzen, was in diesem Fall offensichtlich ist. Marktgeld unterliegt der Geldinflation, erzeugt jedoch keine Preisinflation. Monopolgeld unterliegt in ähnlicher Weise der Geldinflation, erzeugt jedoch Preisinflation – allein

Referenzen

[1] https://en.wikipedia.org/wiki/Stimulus_(economics)

[2] Kapitel: Regressionsfehlschluss

[3] https://de.wikipedia.org/wiki/Seigniorage

[4] https://de.wikipedia.org/wiki/Katallaktik

aufgrund des Produktionsmonopols. Mises verallgemeinert, dass *jede* Geldinflation preisinflationär sei.

> In gleicher Weise steigen auch die Preise, wenn […] die Geldnachfrage sinkt, weil eine allgemeine Tendenz zur Verminderung der Bargeldbestände besteht. Das durch eine solche „Enthortung" zusätzlich verausgabte Geld bewirkt eine Tendenz zu höheren Preisen, auf die gleiche Art wie das, welches aus den Goldminen fließt […]. Umgekehrt sinken die Preise, wenn das Geldangebot sinkt, die Geldnachfrage steigt (z. B. durch eine Tendenz zur „Hortung", der Haltung größerer Bargeldbestände).

Alles Geld gehört immer jemanden. Unter der oben genannten Annahme, dass kein Geld geschaffen wird, bedeutet ein größerer „Bargeldbestand" für eine Person einen geringeren für eine andere Person. Eine zunehmende Geldhortung impliziert lediglich eine geringere gegenwärtige Nachfrage nach Gütern im Verhältnis zur erwarteten zukünftigen Nachfrage. Eine verringerte Hortung bedeutet nur eine erhöhte gegenwärtige Nachfrage nach Gütern. Es ist nicht so, als ob das Geld wieder in die Erde genäht worden wäre. Das „Enthorten" (der Handel mit dem Geld) ist kostenlos, daher ist es nicht dasselbe wie Geld, das „aus den Goldminen fließt".

Ein allgemein erhöhtes Hortungsniveau erweckt den *Eindruck* größeren Reichtums, aber das ist eine Illusion. Um für die Menschen einen Wert zu haben, muss Geld gegen Güter eingetauscht werden, und an diesem Punkt verflüchtigt sich die Illusion. Anders als beim Bergbau ist der Effekt des Enthortens ungleichmäßig. Der Erste, der es tut, erhält den höchsten Tauschwert und der Letzte den niedrigsten. Die Spekulationsstrategie[1] des „Pump and Dump"[2] basiert auf der Ausnutzung dieser Ungleichmäßigkeit. Reichtum wird übertragen, nicht geschaffen.

Referenzen

[1] Kapitel: Spekulativer Konsum

[2] https://de.wikipedia.org/wiki/Pump_and_Dump

Darüber hinaus impliziert erhöhtes Horten eine höhere Zeitpräferenz[1], d. h. das Verhältnis von gehortetem Kapital zu geliehenem Kapital (Kapitalverhältnis[2]), welches sich im Zinssatz widerspiegelt. Dies sind erhöhte Zeitkosten, nicht erhöhte Kapitalwerte. Zum Zeitpunkt des zunehmenden Hortens ist die gleiche Menge an Gütern (Vermögen) vorhanden. Doch diese Zunahme reduziert aufgrund der erhöhten Kapitalkosten die Produktion proportional. Dies führt zu einer dauerhaften und sich steigernden Verringerung des Vermögens, da die verlorene Produktionszeit nicht wieder aufgeholt werden kann, auch nicht durch anschließendes Abbauen von Hortungen. Wenn alles Geld für ein Jahrzehnt gehortet würde (unter der Annahme, dass keine Rückkehr zum Tauschhandel erfolgt), könnte es passieren, dass die Menschen ihre Horte auflösen und dann feststellen, dass ihr Geld aufgrund der dramatischen Verringerung der Warenmenge erheblich an Wert verloren hat.

Unabhängig von Wirtschaftswachstum (oder -kontraktion) impliziert eine Änderung der Nachfrage nach Marktgeld eine proportionale Änderung der Nachfrage nach oder des Angebots von Gütern, die gegen dieses Geld gehandelt werden, im Gegensatz zu anderem Geld oder Tauschhandel. Das Angebot an Gütern ist der Grad, in dem das Geld im Tausch gegen diese Güter akzeptiert wird. Geld weist nur dann einen Geldwert auf, wenn es direkt oder indirekt gegen Dinge mit Gebrauchswert[3] getauscht werden kann, wie dies direkt durch die Geldbeziehung selbst impliziert wird. Der Wert von Geld ergibt sich aus der Bereitschaft der Menschen, es im Handel (d. h. in der Wirtschaft) zu akzeptieren. Angesichts der Fungibilität[4] von Geld bedeutet der Verkauf des Geldes[5] an eine andere Person keine Änderung dieser Akzeptanz.

Referenzen

[1] Kapitel: Zeitpräferenzfehlschluss

[2] Kapitel: Sparverhältnis

[3] https://de.wikipedia.org/wiki/Gebrauchswert

[4] https://de.wikipedia.org/wiki/Fungibilität

[5] Chapter: Dumping-Fehlschluss

Soweit es sich auf Warengeld bezieht, geht dieses Prinzip davon aus, dass die zur Herstellung des Geldes erforderliche Warenmenge konstant bleibt. Der Preis der Waren im Geld wird daher durch die Geldrelation konstant gehalten. Wenn jedoch der Wert, der zur Herstellung eines Warengeldes erforderlichen Waren steigt oder fällt, ist eine entsprechende Senkung oder Erhöhung der Preise des Geldes impliziert. Daher wird die Geldrelation unabhängig von der Nachfrage durch die Änderungsrate der erforderlichen Produktionsfaktoren gesteuert. Solche Änderungen gelten als unvorhersehbar, da sie andernfalls bereits im Preis enthalten sind. Dies stellt insofern einen Spekulationsfehler dar.

Arbeit und Freizeit

Arbeit und Freizeit sind einander ergänzende menschliche Handlungen[1], die mit der Produktion und dem Konsum[2] wirtschaftlicher Güter[3] in Zusammenhang stehen. Arbeit ist der Prozess des Konsums zur Herstellung eines Wirtschaftsgutes (Produktion). Freizeit ist der Prozess des Konsums, der kein wirtschaftliches Gut hervorbringt. Konsum ohne Nutzen ist der Prozess der Verschwendung[4]. Murray Rothbard[5] schreibt in seinem Buch *Mensch, Wirtschaft und Staat*[6]:

> Arbeit bedeutet immer den Verzicht auf Freizeit, ein wünschenswertes Gut
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Dieser subtile Irrtum impliziert, dass sowohl Arbeit als auch Freizeit wirtschaftliche Güter sind. Doch nur Handlungen erzeugen oder konsumieren Güter[7]. Arbeit (Produktion wirtschaftlicher Güter) und Freizeit (Produktion nicht-wirtschaftlicher Güter) sind menschliche Handlungen, die im Laufe der Zeit Güter erzeugen und konsumieren. Im grundlegendsten Sinne impliziert Produktion den Konsum des Körpers des Handelnden, während Konsum dessen Produktion bedeutet.

Referenzen

[1] https://en.wikipedia.org/wiki/Action_axiom
[2] Kapitel: Produktion und Konsum
[3] https://en.wikipedia.org/wiki/Goods_and_services
[4] https://de.wikipedia.org/wiki/Abfall
[5] https://de.wikipedia.org/wiki/Murray_Rothbard
[6] https://mises.org/library/man-economy-and-state-power-and-market/html/p/926
[7] Kapitel: Ausdrucksprinzip

In jeder Stunde wird er seine Anstrengung darauf verwenden, das Gut zu produzieren, dessen Grenzprodukt auf seiner Werteskala am höchsten ist. Wenn er eine Stunde Arbeit aufgeben muss, wird er eine Einheit des Gutes aufgeben, dessen Grenznutzen auf seiner Werteskala am niedrigsten ist. An jedem Punkt wird er den Nutzen des Produktes auf seiner Werteskala gegen den Unnutzen weiterer Arbeit abwägen. Wir wissen, dass der Grenznutzen der durch Anstrengung bereitgestellten Güter sinkt, wenn sich der Aufwand erhöht. Andererseits steigt mit jedem neuen Aufwand der Grenzunnutzen der Anstrengung weiter an. Daher wird ein Mensch seine Arbeit so lang aufwenden, bis der Grenznutzen des Ertrags den Grenzunnutzen der Arbeitsanstrengung übersteigt. Ein Mensch wird die Arbeit einstellen, wenn der Grenzunnutzen der Arbeit größer ist als der Grenznutzen der durch die Anstrengung bereitgestellten Gütervermehrung.

Dann, wenn sein Freizeitkonsum zunimmt, wird der Grenznutzen der Freizeit sinken, während der Grenznutzen der entgangenen Güter zunimmt, bis schließlich der Nutzen der entgangenen Grenzprodukte größer wird als der Grenznutzen der Freizeit und der Akteur seine Arbeit wieder aufnimmt.

Diese Analyse der Gesetze der Arbeitsanstrengung wurde aus den Implikationen des Handlungsaxioms und der Annahme von Freizeit als Konsumgut abgeleitet.

Es ist weder richtig noch notwendig, davon auszugehen, dass Freizeit ein Gut ist, und damit zu implizieren, dass Arbeit ein Anti-Gut ist. Ebenso wenig ist es notwendig, den Kunstgriff des negativen Nutzens („Unnutzens“) zu konstruieren. Wert ist einfach eine Präferenz für einen höheren Nutzen gegenüber einem niedrigeren Nutzen. Sowohl Arbeit als auch Freizeit produzieren Güter mit (positivem) Nutzen.

Es ist die Zeitpräferenz[1], die impliziert, dass der Freizeitnutzen größer ist als der Arbeitsnutzen. Wenn man den Körper einer Person richtigerweise als Eigentum betrachtet, folgt die „Freizeitpräferenz“ direkt aus der Zeitpräferenz. Wie das obige Zitat andeutet, ist dies das Ergebnis eines Tausches von Zeit ohne den eigenen Körper (Arbeitszeit) gegen den Zinsbetrag der den Wert ausgleicht, den man der Zeit mit seinem Körper (Freizeit) zuschreibt.

Zeit, Raum und Güter sind die Faktoren aller Produktion, während Arbeit der Produktionsprozess ist. **Arbeit/Freizeit und Produktion sind unterschiedliche Namen**

Referenzen

[1] Kapitel: Zeitpräferenzfehlschluss

für dieselbe menschliche Handlung. Der Akt des Produzierens ist Arbeit oder Freizeit; der Akt des Arbeitens oder der Freizeitgestaltung ist Produktion. Die Reine Bank[1] liefert das Modell der gesamten Produktion. Dieser Zyklus ist klar ersichtlich im Fall der Selbstständigkeit, die nur ein Beispiel für Produktion ist. Im Fall eines Lohnempfängers gibt es zwei Produzenten, den Arbeitnehmer und den Arbeitgeber.

Ein reiner Lohn empfangender Arbeitnehmer erhält geliehenes Kapital und tauscht es gegen Nahrungsmittel, Bildung und Ausrüstung ein, die er für seinen Job braucht. Ein Teil seines Kapitals wird gehortet und der Rest wird dem Arbeitgeber geliehen. Der Arbeitgeber zahlt dem Arbeitnehmer für die Laufzeit des Darlehens Zinsen (Lohn). Am Ende seines Beschäftigungsverhältnisses erhält der Arbeitnehmer seine abgeschriebene Kreditsumme und seinen Lohn zurück.

Der Lohnsatz gleicht sowohl die Zeitpräferenz für den geliehenen Betrag (Nominalzinssatz) als auch die Kapitalabschreibung während der Laufzeit des Darlehens aus. Der Betrag aus Kapital und Zinsen abzüglich der Abschreibung des reservierten Anteils wird an den Gläubiger des Arbeitnehmers zurückgezahlt. In dem Fall, dass seine Kapitalinvestition aus seinen eigenen Reserven geliehen wird, ist der Arbeitnehmer sein eigener Gläubiger. Der Erlös wird dann gehortet oder in zukünftige Arbeitsleistung (oder anderweitig) reinvestiert.

Ein realer Arbeitgeber und ein realer Arbeitnehmer erhalten jeweils einen marktüblichen Zinssatz. Der Zinssatz des Arbeitnehmers ist sein Lohnsatz abzüglich seiner Produktionskosten. Der Zinssatz des Arbeitgebers ist der Preis, der für das Arbeitsprodukt während der Zeit seiner Herstellung erzielt wird, abzüglich seiner Produktionskosten. Die Produktionskosten des Arbeitgebers sind der Verbrauch seines geliehenen Kapitals, das er über diesen Zeitraum reserviert[2], genau wie beim

Referenzen

[1] Kapitel: Reine Bank

[2] Kapitel: Reserveprinzip

Arbeitnehmer. Der Betrag, um den die Zinsen die Abschreibungen übersteigen, ist der Vermögenszuwachs[1] für beide Parteien.

Der Zinssatz, den beide Produktionsklassen erhalten, ist der gleiche. Der Unterschied in den zurückgezahlten Beträgen ist streng genommen eine Funktion der investierten Kapitalmenge, entweder in die individuelle Produktion (Arbeitnehmer) oder in die Verwaltung der kollektiven Produktion (Arbeitgeber). Die maximale Freizeitbewertung einer Person kann aus dem Lohnsatz abgeleitet werden, welchen sie akzeptiert, indem das implizierte Kapital mit dem Marktzinssatz diskontiert[2] wird.

```
Lohnsatz = Freizeitsatz * (1 + Zinssatz + Körperabschreibungsrate)
```

Der Arbeitnehmer tauscht Freizeit gegen Arbeitszeit ein, und zwar in dem Maße, in dem er den Zinsbetrag höher schätzt als den Wert, den er der Freizeit zuschreibt. Die Freizeitpräferenz ist eine Neuformulierung der Zeitpräferenz, bei der der eigene Körper das wirtschaftliche Gut ist, das der Produktion im Austausch gegen Zinsen zur Verfügung gestellt wird.

Monetärer Wohlstand ist in jungen Jahren im Allgemeinen geringer, was eine höhere Präferenz für Geldzeit bedeutet. Mit der Zeit häuft sich der Wohlstand an und die Zeitpräferenz nimmt ab. Bei der Freizeitpräferenz ist jedoch das Gegenteil der Fall. Geld und der eigene Körper sind nicht dasselbe Eigentum und im Allgemeinen nicht austauschbar. In jungen Jahren ist die Freizeitpräferenz am geringsten. Da der Körper mit dem Alter an Wert verliert, nimmt seine Menge trotz des Geldvermögens ab, was die Freizeitpräferenz erhöht. Das kann schließlich einen höheren als den üblichen Marktzinssatz zum Ausgleich dieser Präferenz erfordern, was zum Ruhestand führt. Geld-Zeitpräferenz und Freizeitpräferenz beeinflussen sich gegenseitig, da sie dazu

Referenzen

[1] Kapitel: Abschreibungsprinzip

[2] https://de.wikipedia.org/wiki/Barwert

neigen, sich in entgegengesetzte Richtungen zu bewegen. In dem Maße, in dem das Ziel der Arbeit darin besteht, den Wohlstand zu steigern, verringert weniger Wohlstand die Freizeitpräferenz und mehr Wohlstand erhöht sie. Auch dies kann zum Ruhestand führen.

Produktion und Konsum

Produktion und Konsum sind die komplementären menschlichen Handlungen[1] der Herstellung und des Konsums von Wirtschaftsgütern[2]. Die menschlichen Rollen als Produzent und Konsument dürfen nicht mit den Handlungen Produktion und Konsum verwechselt werden[3]. Eine Rolle bezieht sich auf eine Absicht, nicht auf eine Handlung. Alle Produzenten konsumieren und alle Konsumenten produzieren. Konsum, der ein wirtschaftliches Gut hervorbringt, ist Produktion, andernfalls ist es entweder ein Prozess der Freizeit[4] oder Verschwendung[5].

Die Reine Bank[6] bietet das Modell der gesamten Produktion. Ein reiner Produzent hat sich Kapital geliehen und verbraucht es bei der Herstellung eines Produktes. Der zu einem beliebigen Zeitpunkt verbrauchte Anteil wurde an die Produktion verliehen. Der zu einem beliebigen Zeitpunkt nicht verbrauchte Anteil wurde für Liquidität reserviert[7]. Das neue Produkt wird verkauft, wodurch Zinsen auf den verbrauchten Teil eingefahren werden, ausgezahlt als Dividende[8]. Die Höhe der Reserve entspricht dem notwendigen Produktionsaufwand, gleich der Liquiditätsreserve der Reinen Bank. **Die Reserve wird nur durch weiteres Fremdkapital wieder aufgefüllt, einschließlich der Reinvestition von Dividenden/Gewinnen.**

Ein realer Produzent wandelt Zeit und Kapital in Zinsen um, und zwar zum Marktpreis des produzierten Produkts, genauso wie eine reale Bank Zinsen zum Marktpreis erhält.

Referenzen

[1] https://en.wikipedia.org/wiki/Action_axiom
[2] https://en.m.wikipedia.org/wiki/Goods_and_services
[3] Kapitel: Abschreibungsprinzip
[4] Kapitel: Arbeit und Freizeit
[5] https://de.wikipedia.org/wiki/Abfall
[6] Kapitel: Reine Bank
[7] Kapitel: Definition der Reserve
[8] https://de.wikipedia.org/wiki/Dividende

Die Bank erhält lediglich die Zinsen eines anderen Produzenten, indem sie dessen Investor ist. Dies zeigt die grundsätzliche Gleichwertigkeit von Krediten als Schulden und Eigenkapital, unabhängig von *gesetzlichen* Unterscheidungen (Steuern).

Ein reiner Konsument hortet Kapital, ohne es der Produktion zu leihen. Das gesamte Kapital ist geliehen und reserviert. Bei 100 % Reserve gibt es keine Zinsen, keine Rendite und schließlich die volle Abschreibung. In diesem Fall wird das geliehene Kapital als Geschenk (Wohltätigkeit[1]) betrachtet. Ein echter Konsument unterliegt zusätzlich Steuern und Subventionen, die die Abschreibungsrate seiner Kapitalreserven entsprechend erhöhen bzw. verringern.

Referenzen

[1] https://de.wikipedia.org/wiki/Wohltätigkeit

Reine Bank

Das Konzept einer Reinen Bank kann bei der allgemeinen Darstellung des Kreditvergabeverhaltens hilfreich sein.

Eine Reine Bank bietet lediglich die folgenden Dienstleistungen an:

- Geld leihen (Schulden von Gläubigern)
- Geld verleihen (Kredit von Schuldnern)
- Geld horten (Reserve)

Die wesentlichen Unterschiede zu einer echten Bank sind:

- Keine staatlichen Eingriffe (freie Bank)
- Keine Betriebskosten (vollkommen Effizient)

Die Bank gehört ihren Gläubigern im Verhältnis ihres Kreditvolumens, wie dies bei jedem Unternehmen der Fall ist. Es gibt große Banken, die ihren Kontoinhabern gehören, wie beispielsweise USAA[1] und Vanguard[2], sodass dies kein Unterschied zu einer echten Bank ist. Weder eine Reine Bank noch eine Echte Bank verfügt über „eigenes Kapital“, das sie verleihen könnte, da das gesamte Kapital in der einen oder anderen Form von Investoren geliehen wird. Das Ziel der Gläubiger besteht darin, ihre Rendite zu maximieren. Das Ziel der Schuldner besteht darin, ihre Zinsaufwendungen zu minimieren.

Referenzen

[1] https://www.usaa.com

[2] https://investor.vanguard.com

Gläubigerkonten sind Geldersatzmittel[1]. Dieser Aspekt unterscheidet die Bank von einem Investmentfonds. Der Geldersatz kann entweder ein Buchgeld[2] oder ein Geldmarktfonds[3] sein. Der Unterschied liegt in der Zuteilung unzureichender Reserven (negative Rendite), wobei erstere nach dem Prinzip „Wer zuerst kommt, mahlt zuerst"[4] und der letztere nach dem Prinzip „die Dollarparität aufgeben"[5] handeln.

Das Fehlen staatlicher Eingriffe ist das allgemeine Konzept des freien Bankwesens[6], bei dem es keine gesetzliche Kontrolle[7], staatliche Versicherung[8], Diskontkapital[9] oder Seigniorage[10] gibt. Sofern nicht anders angegeben, verwendet die Bank Warengeld[11], was die Berechnungen vereinfacht, da keine Preisinflation[12] oder Preisdeflation[13] herausgerechnet[14] werden muss.

Perfekte Effizienz unterscheidet sich von einer Echten Bank nur in der Rendite, da im Betrieb nichts verbraucht wird. Alle Erträge sind eine Folge der Zeitpräferenz[15]. Es wird ein einheitlicher Zinssatz angenommen, da Arbitrage[16] eine Ausgabe darstellt.

Referenzen

[1] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[2] https://de.wikipedia.org/wiki/Buchgeld

[3] https://de.wikipedia.org/wiki/Geldmarktfonds

[4] https://de.wikipedia.org/wiki/Bankansturm

[5] https://en.wikipedia.org/wiki/Money_market_fund#Breaking_the_buck

[6] https://de.wikipedia.org/wiki/Free_Banking

[7] https://de.wikipedia.org/wiki/Federal_Reserve_System

[8] https://www.fdic.gov

[9] https://en.wikipedia.org/wiki/Discount_window

[10] https://de.wikipedia.org/wiki/Seigniorage

[11] Kapitel: Taxonomie des Geldes

[12] https://de.wikipedia.org/wiki/Inflation

[13] https://de.wikipedia.org/wiki/Deflation

[14] Kapitel: Inflationsprinzip

[15] Kapitel: Zeitpräferenzfehlschluss

[16] https://de.wikipedia.org/wiki/Arbitrage

Demurrage[1] ist die Ausgabe für die Geldaufbewahrung. Die Kostenrate (einschließlich Demurrage) der Reinen Bank ist 1.

Reservekapital[2] ist das Geld, in welchem Kredite und Schulden beglichen werden[3] (null Fälligkeit[4]). Abwertung[5] sind die Opportunitätskosten[6], die entstehen, wenn das Kapital nicht verliehen wird, auch bekannt als „Cash Drag“. Zinsbeziehungen gehen von einer einzigen Zinsperiode[7] mit einem Zinssatz über dieser Periode aus. Diese Vereinfachung der Darstellung ist für implizite Zusammenhänge bedeutungslos.

Angesichts der vorangegangenen Definition einer Reinen Bank sind die folgenden Zusammenhänge absolut.

```
Reserviert = Geliehen - Verliehen
Liegegeld = Liegegeldzinsrate * Reserviert
Abwertung = Zinsrate * Reserviert
Zinsen = Zinsrate * Verliehen
Rendite = Kostenverhältnis * Zinsen
```

Bei der Reinen Bank bestimmt die Reservequote[8] vollständig die Kapitalquote[9], die Schuldenquote[10] und die Sparquote.

Referenzen

[1] https://de.wikipedia.org/wiki/Umlaufgesichertes_Geld

[2] Kapitel: Definition der Reserve

[3] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)

[4] https://de.wikipedia.org/wiki/Fälligkeit

[5] Kapitel: Abschreibungsprinzip

[6] https://de.wikipedia.org/wiki/Opportunitätskosten

[7] https://de.wikipedia.org/wiki/Zinseszins

[8] https://de.wikipedia.org/wiki/Mindestreserve

[9] https://de.wikipedia.org/wiki/Solvabilität

[10] https://en.wikipedia.org/wiki/Debt_ratio

Reservequote

```
Reservequote = Reserviert / Geliehen
Reservequote = (Geliehen - Verliehen) / Geliehen
```

Kapitalquote

```
Kapitalquote = Reserviert / Verliehen
Kapitalquote = (Geliehen - Verliehen) / Verliehen
```

Schuldenquote

```
Schuldenquote = Geliehen / Reserviert
Schuldenquote = Geliehen / (Geliehen - Verliehen)
```

Sparquote

```
Sparquote = Verliehen / Reserviert
Sparquote = Verliehen / (Geliehen - Verliehen)
```

Bilanz

Die Reine Bank hat keine Verbindlichkeiten, sondern nur Eigenkapital.

Bankvermögen	Eigenkapital
Verliehen + Reserviert	Geliehen

Rendite

Die Rendite des Gläubigers ist zusätzlich eine Funktion des Zinssatzes. Die Rendite des Gläubigers ist aufgrund des Cash Drag, der notwendigen Kosten für die Abhebung auf Nachfrage, geringer als der Zinssatz des Schuldners. Um diesen Aufwand zu reduzieren, werden in echten Bankverträgen[1] normalerweise zeitliche Beschränkungen aufgenommen. Beispielsweise kann jede Abhebung von einem verzinslichen US-Bankkonto per Gesetz um sieben Tage verzögert werden. Der Gläubiger kann den Cash Drag[2] nur durch direkte Investitionen (d. h. ohne Erfüllungsgarantien) vermeiden.

```
Rendite = Zinsrate * Verliehen / Geliehen
```

Wie im Sparverhältnis[3] dargestellt, bestimmen die individuellen Kapitalquoten den Marktzinssatz vollständig. Wenn wir jeden Menschen als eine Reine Bank betrachten, wird klar, dass die Kapitalquote den Zinssatz bestimmt. Eine Kapitalquote von 0% für alle Menschen bedeutet, dass Kapital kostenlos ist und keine Rendite bringt. Bei steigender Kapitalquote steigt der Zinssatz entsprechend. Bei voller Hortung sind die Kapitalkosten „unendlich“ – es kann kein Kapital für die Produktion beschafft werden.

Die Annahme der Geldrelation[4] ist, dass der Preis proportional zum Verhältnis von Nachfrage und Angebot ist. Aber wie die Sparrelation zeigt, stehen Angebot und

Referenzen

[1] https://www.chase.com/content/dam/chase-ux/documents/personal/checking/deposit-account-agreement.pdf

[2] https://www.investopedia.com/terms/p/performance_drag.asp

[3] Kapitel: Sparverhältnis

[4] Kapitel: Inflationsprinzip

Nachfrage nach Kapital in einer Nullsummenbeziehung. Eine Zunahme der Hortung bedeutet eine entsprechende Abnahme der Kreditvergabe und umgekehrt eine Zunahme. Daher sind weder die Kapitalquote noch der Zinssatz linear in Bezug auf die Veränderung des gehorteten (oder verliehenen) Betrags. Dies hat einige dazu veranlasst, nach einem „Goldenen Schnitt"[1] zu suchen. Angesichts der Subjektivität des Wertes ist dies jedoch letztlich ein sinnloses Unterfangen.

Doch die Kapitalquoten bestimmen den Zinssatz vollständig. Da jeder individuell versucht, einen goldenen Schnitt auf der Grundlage seiner eigenen Präferenzen zu erzielen, ergibt sich daraus der Marktzinssatz. Ersetzt man den Zinssatz durch die Kapitalquote, zeigt sich die Auswirkung der Reservierung auf die Reine Bank, unter der zusätzlichen Annahme, dass jeder als Reine Bank und mit derselben Kapitalquote operiert. Die Kapitalquote beinhaltet die Wertminderung gegenwärtiger Güter, die bei Geld das Liegegeld ist. Das Liegegeldverhältnis der Reinen Bank beträgt 1, also fällt dieses heraus.

```
Rendite = (Reserviert * Liegegeldquote / Verliehen) * (Verliehen /
Geliehen)
Rendite = (Reserviert / Geliehen) * Liegegeldquote
Rendite = Reserviert / Geliehen
```

Die Rendite der Investitionen der Reinen Bank wird zur Reservequote. Dies bedeutet nicht, dass eine einzelne Reine Bank ihre eigene Rendite durch Festlegung ihrer Kapitalquote festlegen kann. Es spiegelt lediglich wider, dass die Marktkapitalquote die Kapitalrendite bestimmt. Wenn *alle Kreditgeber* ihre derzeitige Kapitalquote verdoppeln würden, würden sich ihre Renditen zwangsläufig verdoppeln, da sich die Kapitalkosten und damit auch die Rendite verdoppeln würden.

Referenzen

[1] https://en.wikipedia.org/wiki/Golden_Rule_savings_rate

Echte Banken

Die unabhängigen Kapitalquoten aller Menschen, basierend auf der individuellen Zeitpräferenz, bestimmen den Marktzinssatz. Die obige Ersetzung der Eigenkapitalquote der Bank als Zinssatz scheint zu implizieren, dass die Bank den Zinssatz festlegt. Dies ist jedoch dem Konzept der Zeitpräferenz inhärent. Eine Bank kann jedes beliebige Zinsniveau festlegen. Bei Echten Banken wird nicht davon ausgegangen, dass der Markt gehorcht, daher werden Marktzinsen und damit Marktrenditen angenommen.

```
Marktrendite = Marktzinssatz * (Verliehen / Geliehen)
Marktrendite = Marktkapitalquote * (Verliehen / Geliehen)
```

Die Freie Bank unterscheidet sich von der Reinen Bank auch durch die Betriebskosten, die die Rendite direkt reduzieren.

```
Freie-Bank-Rendite = Marktrendite * Kostenquote
```

Die Echte Bank unterscheidet sich von der Freien Bank nur durch die Steuern (einschließlich der Kosten für Regulatorik), die die Rendite direkt reduzieren.

```
Echte-Rendite = Freie-Bank-Rendite * Steueraufwandsquote
```

Die Zentralbank (der Staat) unterscheidet sich von der Echten Bank nur durch die Subventionen der Steuerzahler (einschließlich diskontierter Kredite), die die Rendite direkt erhöhen.

```
Zentrale-Rendite = Echte-Rendite * Subventionseinkommenquote
```

Wenn die Steuer die Seigniorage des Bankgeldes beinhaltet, muss die Fisher-Gleichung[1] oben angewendet werden, um den Zinssatz von einem Nominalzinssatz in einen Realzinssatz umzuwandeln. Außer der Steuer ist keine andere Änderung impliziert, die oben von der Echten Bank verrechnet wird. Diese Steuer ist im Allgemeinen die Quelle der Subvention, die oben von der Zentralbank abgerechnet wird.

Jeder Mensch oder jede Gesellschaft von Menschen ist eine Echte Bank, und der Staat ist eine Zentralbank. Eine Echte Bank erbringt die Dienstleistung liquider Investitionen, ein Wirtschaftsgut[2]. Die Produktionskosten sind die Abschreibung ihrer Reserven. Dies ist das Modell aller Produktion.

Referenzen

[1] https://de.wikipedia.org/wiki/Fisher-Gleichung

[2] https://de.wikipedia.org/wiki/Gut_(Wirtschaftswissenschaft)

Sparverhältnis

Zeitpräferenz[1] ist die katallaktische[2] Annahme, dass der Mensch gegenwärtige Güter gegenüber zukünftigen Gütern bevorzugt. Es ist allgemein anerkannt, dass sich die Zeitpräferenz im Zinssatz widerspiegelt. Murray Rothbard[3], schreibt in seinem Buch *Mensch, Wirtschaft und Staat*[4]:

> Die Höhe des reinen Zinssatzes wird durch den Markt für den Tausch gegenwärtiger Güter gegen zukünftige Güter bestimmt, ein Markt, der, wie wir sehen werden, viele Teile des Wirtschaftssystems durchdringt. […] Wenn also auf dem Zeitmarkt 100 Unzen Gold gegen die Aussicht getauscht werden, in einem Jahr 105 Unzen Gold zu erhalten, dann beträgt der Zinssatz ungefähr 5 Prozent pro Jahr. Dies ist der Zeitdiskontsatz von zukünftigem zu gegenwärtigem Geld. […] Der reine Zinssatz ist dann der gängige Zeitdiskontsatz, das Verhältnis des Preises gegenwärtiger Güter zu dem zukünftiger Güter.
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Es ist jedoch die individuelle Kapitalquote[5] die den Zinssatz *bestimmt*. Das Zinsverhältnis ist das Verhältnis zwischen dem zukünftigen und dem gegenwärtigen Warenpreis. Es ist die Marktpreisprämie, die erforderlich ist, um einen Eigentümer für die Zeit ohne dessen Ware zu entschädigen – oder der Preis der Zeit. Wie bei allen Preisen wird er vollständig durch individuelle Präferenzen bestimmt, in diesem Fall durch Zeitpräferenzen, ausgedrückt[6] als individuelle Handelsgeschäfte.

Die Zeitpräferenz eines Individuums kann als Verhältnis des Preises seines Hortes zu dem seiner vergebenen Kredite dargestellt werden. Zusammen ergeben diese Beträge seine Ersparnisse. Indem man einen Teil seines Hortes gegen seinen zukünftigen Wert

Referenzen

[1] Kapitel: Zeitpräferenzfehlschluss

[2] https://de.wikipedia.org/wiki/Katallaktik

[3] https://de.wikipedia.org/wiki/Murray_Rothbard

[4] https://mises.org/library/man-economy-and-state-power-and-market/html/p/989

[5] https://de.wikipedia.org/wiki/Solvabilität

[6] Kapitel: Ausdrucksprinzip

eintauscht, drückt man aus, dass ihm der zukünftige Betrag mehr wert ist als der gegenwärtige. Umgekehrt drückt man die entgegengesetzte Bewertung aus, indem man dies nicht tut.

Ein Hort ist die Möglichkeit zu investieren (zu verleihen) und eine Investition ist die Möglichkeit zu konsumieren. Das eine wird gegen das andere getauscht, bis dadurch kein weiterer Wertzuwachs mehr erzielt wird. Durch eine Investition schätzt man den zukünftigen Betrag höher ein als den gegenwärtigen, nicht investierten Betrag. Durch eine Nichtinvestition schätzt man den gegenwärtigen, nicht investierten Betrag höher ein als den zukünftigen Betrag. Wäre dies nicht der Fall, würde das Investitionsniveau entsprechend niedriger bzw. höher sein. Diese Bewertung, die sich als Tausch manifestiert, ist Ausdruck der eigenen Zeitpräferenz.

> Vielleicht sind in Diskussionen über den Zinssatz mehr Irrtümer begangen worden als in der Behandlung irgendeines anderen Aspekts der Ökonomie. Es dauerte lange, bis die Ökonomie die entscheidende Bedeutung der Zeitpräferenz bei der Bestimmung des reinen Zinssatzes erkannte; es dauerte sogar noch länger, bis die Ökonomen erkannten, dass die Zeitpräferenz der einzige bestimmende Faktor ist. Die Zurückhaltung gegenüber einer monistischen Kausalinterpretation plagt die Ökonomie bis heute.

Der Marktzinssatz wird nicht durch den *Einzelnen* kontrolliert. Der Einzelne kontrolliert seine Kapitalquote angesichts des Marktzinssatzes. Die Kapitalquote ist es, wie individuelle Zeitpräferenz *ausgedrückt* wird. Der Zinssatz gibt an, wie diese Präferenzen durch den Markt *bepreist* werden.

Das folgende vertikale Balkendiagramm bietet ein Beispiel für die Ersparnisse einer Einzelperson.

Jeder ordinale Zuwachs stellt einen marginalen Wertzuwachs dar. Die Symbole H, P und T stellen jeweils Zuwächse des Hort-, Barwert- und Zeitwertes dar. Der Hortwert ist der Barwert einer nicht verliehenen Einheit. Der Barwert ist der Wert einer verliehenen Einheit, wenn sie nicht verliehen worden wäre. Der Zeitwert ist der erwartete Nettowert (Kreditbetrag + Zinsen) der verliehenen Einheit über einen bestimmten Zeitraum zum Marktzinssatz für diesen Zeitraum.

Jeder vertikale Balken auf der horizontalen Achse repräsentiert eine Geldeinheit, doch jede Einheit hat für den Besitzer einen anderen Grenzwert, was eine Folge des Grenznutzens[1] ist. Dieser Wert wird auf der vertikalen Achse als Balkenhöhe

Referenzen

[1] https://de.wikipedia.org/wiki/Grenznutzen

ausgedrückt. Man sollte Wert nicht mit Preis verwechseln. Der Wert jeder im Besitz befindlichen Einheit steigt, wenn der Hort abnimmt, und daher sinkt der Nettowert bei gleichem Zinssatz (Preis für Geld[1]) mit der Abnahme des Hortes, bis er negativ wird (wo nichts mehr verliehen wird).

Die Zeitpräferenz des Einzelnen wird durch seine Bewertung zwischen den Grenzeinheiten „c“ (die nächste potenziell zu verleihende Einheit) und „d“ (die letzte verliehene Einheit) veranschaulicht. Der Barwert[2] der ersteren ist höher als ihr potenzieller Zeitwert[3] ausgleichen kann, daher wird sie nicht verliehen. Der Barwert der letzteren ist höher als der potenzielle Zeitwert, daher wird sie verliehen. Steigt der Marktzinssatz so, dass die Renditesteigerung bei der Kreditvergabe „c“ den Kardinalwertzuwachs von „b“ (d. h. Diagrammzelle „b19“) übersteigt, wird „c“ verliehen. Fällt der Marktzinssatz so, dass die Renditeminderung bei „d“ „c18“ übersteigt, wird das Darlehen von „d“ getilgt.

Die Gesamtersparnisse betragen 20 Einheiten (Einheiten „a“ bis „t“). Die Gesamthortung beträgt 3 Einheiten („a“ bis „c“). Die Gesamtkreditvergabe beträgt 17 Einheiten („d“ bis „t“). Die Eigenkapitalquote des Einzelnen beträgt daher 3/17 (~17,65 %), im Diagramm als vertikale Linie zwischen den Einheiten „c“ und „d“ dargestellt. Die Opportunitätskosten[4] der Hortung betragen 3 Einheiten x Marktzinssatz. Die Rendite der Kreditvergabe beträgt 17 Einheiten x Marktzinssatz.

Da Wert subjektiv ist[5], ist es wichtig zu beachten, dass in diesem Zusammenhang ausschließlich die individuelle Bewertung des Zinsbetrags von Bedeutung ist. Der Marktzinssatz erhöht seine Ordinalbewertung der verliehenen Einheiten zwischen „18“

Referenzen

[1] Kapitel: Taxonomie des Geldes

[2] https://de.wikipedia.org/wiki/Barwert

[3] https://de.wikipedia.org/wiki/Zeitwert_des_Geldes

[4] https://de.wikipedia.org/wiki/Opportunitätskosten

[5] https://en.wikipedia.org/wiki/Subjective_theory_of_value

und „19“. Das Diagramm stellt den Marktzins daher als horizontale Linie zwischen diesen Inkrementen dar.

Nur die Entscheidung, Geld zu verleihen oder nicht zu verleihen, drückt Zeitpräferenz aus. Die Entwertung erfolgt bei dem, was gehortet wird, nicht bei dem, was verliehen wird. Wie im Abschreibungsprinzip[1] gezeigt, ist Horten Konsum. Die allgemeine Auffassung, dass ein Handel von „Produzent“ zu „Konsument“ Konsum darstellt, ist ein klarer Irrtum. Man kann seine Abschreibungsrate senken und dadurch die Haltbarkeit seines Horts verlängern, **aber um dies als Zeitpräferenz widerzuspiegeln, muss man seinen Kreditzinssatz ändern.**

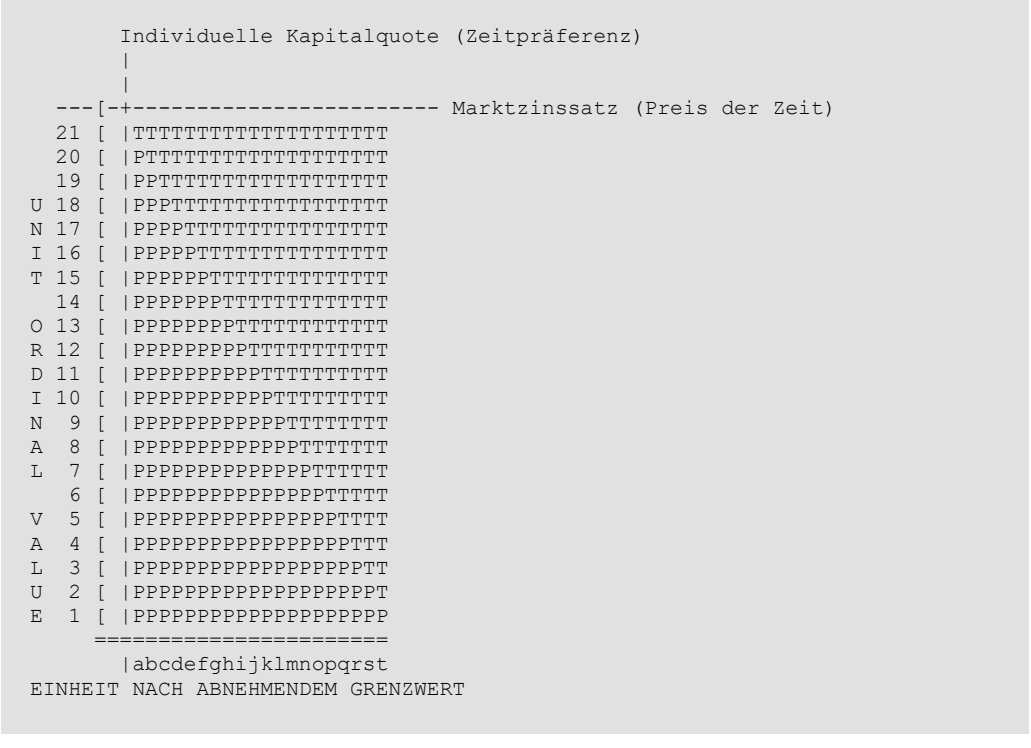
Referenzen

[1] Kapitel: Abschreibungsprinzip

Beachten Sie, dass im Vergleich zur vorherigen Grafik eine Senkung des Zinssatzes um den Wert des 18. Ordnungsinkrements bedeutet, dass eine Einheit weniger verliehen wird.

Dies gilt für jede Zinssenkung bis hinunter zu dem Zinssatz, bei dem der Einzelne nicht mehr leiht.

Gleiches gilt für den Fall, dass der Einzelne sein gesamtes Kapital verleiht.



Spekulativer Konsum

Die Katallaktik[1] definiert zwei Arten der Kapitalnutzung, Konsum und Produktion. Produkte werden produziert und konsumiert. Produktion, oder die Herstellung von Produkten, erfordert Zeit und dafür eingespartes Kapital (Investition). Der Konsum erfordert ebenfalls Zeit und dafür eingespartes Kapital (Hort).

Menschliche Energie kann in der Freizeit oder bei der Arbeit[2] verbraucht werden. Wobei der Wertverlust der gespeicherten menschlichen Energie einen Produktionsfaktor (Kosten) darstellt. In beiden Fällen ist die Umwandlung dieser potenziellen Energie[3] in Arbeit[4] ein Verbrauch von gespeichertem Kapital. Arbeit kann Nahrung produzieren, die ein Mensch sofort verzehren kann. Das ist eine absolute Subsistenzwirtschaft[5], bei der die einzige Ersparnis, die im eigenen Körper gespeicherte potenzielle Energie ist. Das Produkt aus Arbeit, Zeit und naturgegebenen[6] Faktoren wird kontinuierlich verbraucht, entweder zur Produktion (z.B. Beeren pflücken) oder in der Freizeit (z.B. im Schlaf). Dies wird manchmal als ein Leben „von der Hand in den Mund" bezeichnet. Das bei diesem Prozess gesparte Eigentum ist der eigene Körper des Menschen. Ein Kind beginnt sein Leben mit potenzieller Energie, die es von seiner Mutter geschenkt bekommen hat.

Ersparnisse sind daher die einzige Quelle von Produktion und Freizeit. Es stellt sich also die Frage, wofür die Ersparnisse verwendet werden. Selbst im Fall von verdauter Nahrung bleibt diese Frage bestehen. Für die Produktion eingesetztes Kapital wird gegen das Eigentum an dem eingetauscht, was letztendlich produziert wird. Dieses Eigentum

Referenzen

[1] https://de.wikipedia.org/wiki/Katallaktik

[2] https://mises.org/online-book/man-economy-and-state-power-and-market/1-fundamentals-human-action/8-factors-production-labor-versus-leisure

[3] https://de.wikipedia.org/wiki/Potentielle_Energie

[4] https://de.wikipedia.org/wiki/Arbeit_(Physik)

[5] https://de.wikipedia.org/wiki/Subsistenzwirtschaft

[6] https://mises.org/online-book/man-economy-and-state-power-and-market/1-fundamentals-human-action/9-formation-capital

an einem zukünftigen Gut wird als „Sparinvestition“ (oder einfach „Investition“) bezeichnet. Kapital, das nicht für die Produktion eingesetzt wird, wird als „Sparvorrat“ (oder einfach „Hort“) bezeichnet. Ersparnisse sind die Summe des gehorteten und des investierten Kapitals. Der Prozess, gehortetes Kapital für Investitionen oder Freizeit einzusetzen, wird als „Enthortung“[1] bezeichnet.

> Nachdem er seine Dienstleistungen verkauft hat, bezieht er sein Geldeinkommen aus der Produktion und vergrößert damit seine Geldmenge. Dieses Einkommen teilt er dann zwischen Konsum und Sparen bzw. Investitionen auf. Wir gehen davon aus, dass weder Horten noch Enthorten stattfindet.
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Die Katallaktik befasst sich mit menschlichen *Handlungen* und lehnt die Analyse menschlicher *Gedanken* ausdrücklich ab. Gedanken sind subjektiv und drücken sich objektiv nur durch die Durchführung eines Handels aus. Dieses Prinzip verkörpert sich in der Theorie des subjektiven Wertes[2]. Da Zeit ein notwendiger Faktor sowohl für Produktion als auch für Freizeit ist, wird *angenommen* sie hätte einen objektiven Wert. Es gibt keine Hinweise darüber, ob Ersparnisse für die Produktion oder die Freizeit verwendet werden sollen, bis sie abgebaut werden. Man kann Ersparnisse für die Produktion bevorzugen, dann aber verschlafen und die Ersparnisse in der Freizeit verbrauchen. Ähnlich kann man Äpfel generell bevorzugen, aber einen Apfel gegen eine Orange tauschen. Der einzige objektive Ausdruck einer Präferenz ist ein Tausch, einschließlich des Tausches von Ersparnissen gegen Konsum durch Produktion oder Freizeit. Da es nicht auf die Produktion angewendet wird, wird gehortetes Kapital als „unproduktiv“ bezeichnet, genau wie eine Person, die nicht in der Produktion tätig ist.

Horten ist eine notwendige Folge von Unsicherheit. Mit zunehmender Unsicherheit neigen die Menschen dazu, ihr Sparniveau zu steigern, was entweder ihre Freizeit oder ihre Produktion einschränkt. Dadurch kann ihr gehortetes Kapital in Zukunft für beides

Referenzen

[1] https://mises.org/library/man-economy-and-state-power-and-market/html/p/992

[2] https://en.wikipedia.org/wiki/Subjective_theory_of_value

eingesetzt werden. Unproduktives Kapital verursacht jedoch Zeitkosten. Zeit ist objektiv wertvoll. Die Möglichkeit, das Kapital in der Produktion einzusetzen, wurde gegen mehr Sicherheit eingetauscht. Dies sind die Opportunitätskosten[1] der Sicherheit, ein Aufwand. Sowohl bei produktiver als auch unproduktiver Nutzung von Kapital werden Chancen gegen Sicherheit eingetauscht. Der Hort wird als „Liquidität" bezeichnet und ist nur aufgrund der Tatsache der Unsicherheit[2] notwendig.

Wie in Sparverhältnis[3] gezeigt, ist das Verhältnis zwischen gehorteten und investierten Ersparnissen ein Ausdruck der menschlichen Zeitpräferenz[4]. Wie bei allen Bewertungen ist auch die Sicherheit relativ zu den Opportunitätskosten subjektiv. Auch wenn Zeit einen objektiven Nutzen hat (d.h. mehr Zeit ist mehr wert als weniger), bleibt ihr Wert relativ und subjektiv. Doch wie bei allen Bewertungen ergibt sich daraus im Zeitverlauf ein objektiver Preis für Kapital, der durch Tausch ausgedrückt und als Zinssatz bezeichnet wird. Zinsen sind sowohl die Kapitalrendite als auch die Kapitalkosten. Opportunitätskosten sind der Verlust an Produktionsgewinn, der durch die Kapitalhortung entsteht, gemessen am Zinssatz.

Ein Sparvorrat repräsentiert die subjektive Einschätzung, dass er im Laufe der Zeit mehr wert ist als die Opportunitätskosten, die er im Laufe dieser Zeit darstellt. Dies nennt man „Spekulation". Sie ist der Ausdruck einer Präferenz, ein Gut zu besitzen, anstatt sich davon zu trennen, wobei seine Kosten anhand der entgangenen Zinsen gemessen werden. Die Möglichkeit, den Kapitalvorrat (Hort) über den Sparzeitraum zu investieren, ist für immer verloren. Mit anderen Worten, die Handlung, kein Kapital zu investieren, ist der Verbrauch von Kapital. Wenn alles Kapital gehortet ist, wird kein neues Kapital produziert und schließlich ist alles Kapital verbraucht.

Referenzen

[1] https://de.wikipedia.org/wiki/Opportunitätskosten

[2] https://mises.org/wire/problem-hoarding

[3] Kapitel: Sparverhältnis

[4] Kapitel: Zeitpräferenzfehlschluss

Wie die Spekulation „gerechtfertigt“ wird, ist für diese Unterscheidung nicht relevant, da Wert subjektiv ist. Dennoch ist ein gewisses Maß an Horten aufgrund der Unsicherheit (d. h. der Zukunft) notwendig. Eine Präferenz für Kapital in der Gegenwart gegenüber mehr Kapital in der Zukunft drückt sich immer im Horten aus. Man kann sicherlich Geld auf einem Niveau horten, das über die Liquidität hinausgeht, die zur Kompensation der Unsicherheit gedacht ist. Beispielsweise kann man Geld horten, um den Unterhaltungswert von Glücksspielen[1] zu erhalten. Die Opportunitätskosten sind in diesem Fall Unterhaltungskosten. Man kann Kapital horten, um einen Verkauf zu terminieren[2]. Die Opportunitätskosten werden in diesem Fall „Cash Drag” genannt. Es spielt keine Rolle, ob die Person einen Nettogewinn erwartet oder realisiert, das Horten stellt zwangsläufig eine Ausgabe dar – denn Zeit hat einen Wert.

Zeitpräferenz wird jedoch manchmal fälschlicherweise als Beziehung zwischen Konsum und Sparen interpretiert. Dies wird oft vage als „aufgeschobener Konsum“ oder „verzögerte Befriedigung“ beschrieben. Doch wie gezeigt wurde, ist Horten Konsum. Der Konsum wurde nicht aufgeschoben; die Befriedigung wurde nicht verzögert. Der Ausgleich von Unsicherheit ist Befriedigung (Seelenfrieden), Unterhaltung ist Befriedigung (Freizeitbeschäftigung), der potenzielle Gewinn bei erfolgreichem Markttiming ist Befriedigung (Vorhersage eines besseren Preises). All dies verbraucht Kapital. Der Unterschied, den das Konzept der Zeitpräferenz macht, besteht im Austausch von Kapital über einen bestimmten Zeitraum gegen Zinsen. Bei einer Spekulation gibt es keinen solchen Handel.

Das gesamte Vermögen (Ersparnisse) einer Person wird entweder gehortet oder investiert. Das Horten lässt dieses Vermögen mit der Zeit schwinden. Autos verschleißen, Lebensmittel werden in Energie umgewandelt, Möbel verschleißen, Kapital verfällt. Bei Geld ist das nicht anders, es verfällt in einem Hort sowohl aufgrund

Referenzen

[1] https://en.wikipedia.org/wiki/Game_of_chance

[2] https://en.wikipedia.org/wiki/Market_timing

seiner Haltekosten[1] als auch seiner Opportunitätskosten. Der Gegenstandswert[2] des Geldes wird immer gegenüber seinem zukünftigen Wert diskontiert. Dies wird als „Zeitwert des Geldes" bezeichnet. Durch die Ausgabe des zukünftigen Wertes verliert das gehortete Geld während der Hortungszeit tatsächlich um den Betrag des Abschlags an Wert.

Wie im Abschreibungsprinzip[3] gezeigt, ist der Kauf von Waren kein Konsum. Es gibt keinen tatsächlichen Konsum, außer in dem Maße, in dem Eigentum an Wert verliert (verfällt). Daher gibt es keinen Unterschied zwischen dem Aufschieben des Kaufs von Waren und dem Kauf derselben. Dies ist nur ein Tausch einer Art von Eigentum gegen eine andere, und beide unterliegen dem Wertverlust. Zeitpräferenz ist kein Unterschied zwischen Konsum und Sparen, sondern ein Unterschied zwischen Horten und Investieren.

Unternehmertum bringt zwangsläufig Spekulation und Investitionen mit sich. Für die Produktion wird Kapital benötigt, und der Unternehmer spekuliert auf den Preis des zu produzierenden Produkts. Diese Spekulation auf ein zukünftiges Gut ist die unvermeidliche Nebenwirkung der Produktion von Produkten ohne festgelegten Preis. Unternehmertum ist daher „spekulative Produktion", während die Abwertung eines gegenwärtigen Gutes „spekulativer Konsum" ist. Da jede Schätzung zukünftiger Preise fehlerbehaftet ist, sind alle Investitionen bis zu einem gewissen Grad unternehmerisch. Investition ist spekulative Produktion und Horten ist spekulativer Konsum. Dies zeigt sich daran, dass, wenn alles Kapital gehortet wird, keine Produktion stattfindet.

Die obige Diskussion unterscheidet zwischen produktiver und konsumtiver Nutzung von Kapital im Kontext einer einzelnen Person. Der Einfachheit halber haben wir nur den Freizeitkonsum (d. h. den Konsumvorrat eines Konsumenten) besprochen und den

Referenzen

[1] https://en.wikipedia.org/wiki/Cost_of_carry

[2] https://de.wikipedia.org/wiki/Barwert

[3] Kapitel: Abschreibungsprinzip

produktiven Konsum (d. h. den Hort eines Produzenten) vermieden. Während eine einzelne Person sowohl Konsument als auch Produzent sein kann, muss ein Produzent bei der Produktion auch konsumieren. Da die Begriffe dadurch überladen werden, ist es einfacher, sich die Investition einer Person als Investition in das Produktionsgeschäft einer anderen Person vorzustellen.

Das *Ziel* einer Person ist die Freizeit, während das Ziel eines Unternehmens die Produktion ist. Beide Ziele sind konsumtiver Natur, doch der Konsum im Kontext eines Unternehmens dient der Produktion, nicht der Freizeit. Genau wie jede Person muss ein Unternehmen sein Verhältnis von Vorräten zu Investitionen basierend auf Zeitpräferenzen bestimmen. Die Investitionen eines Unternehmens können nicht in seine eigene Produktion fließen, ebenso wie die Investitionen einer Person nicht in ihre eigene Freizeit fließen können, da beides zirkulär wäre. Ein Unternehmen erwirbt Vermögenswerte und entwertet sie im Laufe der Zeit. Obwohl diese umgangssprachlich oft als Investitionen bezeichnet werden, zahlt sich ein Unternehmen selbst keine Zinsen. Diese Vermögenswerte sind gehortetes Kapital im Prozess des Konsums mit dem Ziel der Produktion. Das verbleibende Kapital wird in andere Unternehmen investiert, beispielsweise in Investmentfonds oder verzinsliche Bankkonten. Da jede Person und jedes Unternehmen einen Teil[1] seines Kapitals hortet und den Rest investiert, weitet sich der Kredit[2] auf Geld[3] in Abhängigkeit zur Zeitpräferenz aus.

Die Vorstellung, dass eine Person sowohl Konsument als auch Produzent ist, wirft die kategorische Frage der Arbeit auf. Obwohl alle Menschen konsumieren müssen, sind die meisten auch Produzenten. Eine Person, die einer Lohnarbeit nachgeht, ist ein Produzent. Ein Angestellter[4] investiert Kapital in seine Person (z.B. Bildung, Reputation, Nahrung) und investiert Zeit ohne sein Humankapital, wenn er sich nicht seinem Ziel der

Referenzen

[1] Kapitel: Vollreservefehlschluss

[2] Kapitel: Fehlschluss der Kreditausweitung

[3] Kapitel: Taxonomie des Geldes

[4] https://de.wikipedia.org/wiki/Salaryman

Freizeit widmet. Gehalt und damit verbundene Leistungen sind seine Kapitalrendite. Aufgrund der Arbeitskonkurrenz strebt diese Rendite die Höhe der Verzinsung seines Marktwerts während der Arbeitszeit an.

Spekulation ist eine notwendige Folge von Fehlern, die sowohl dem Konsum als auch der Investition innewohnen. Horten ist konsumtiv und Investieren ist produktiv. Das ökonomische Konzept der Zeitpräferenz ist insbesondere die Unterscheidung zwischen Horten und Investieren. Dies wird deutlich in der Identitätsbeziehung zwischen Zeitpräferenz und wirtschaftlichem Interesse. **Ein höheres Verhältnis von Horten zu Investitionen spiegelt eine höhere Zeitpräferenz wider und impliziert eine geringere Produktion.**

Subjektives Inflationsprinzip

Die Preisinflation[1] auf dem freien Markt ist ausschließlich die Folge persönlicher Präferenzen und kann daher nicht aus irgendetwas anderem abgeleitet werden.

- Güterpreise werden subjektiv bestimmt. (Theorie des subjektiven Wertes[2])
- Zeitpräferenz bestimmt die Ausweitung[3] des Kredits gegenüber dem Geld. (Axiom der Zeitpräferenz[4])
- Geldschöpfung[5] ist nicht preisinflationär. (Inflationsprinzip[6])

Dies ließe sich einfacher aus der Definition des freien Marktes ableiten, der ausschließlich eine Folge persönlicher Präferenzen ist.

Referenzen

[1] https://de.wikipedia.org/wiki/Inflation

[2] https://en.m.wikipedia.org/wiki/Subjective_theory_of_value

[3] Kapitel: Fehlschluss der Kreditausweitung

[4] Kapitel: Zeitpräferenzfehlschluss

[5] Kapitel: Taxonomie des Geldes

[6] Kapitel: Inflationsprinzip

Zeitpräferenzfehlschluss

Es gibt eine Theorie, dass eine niedrigere Zeitpräferenz[1] besser ist als eine höhere, da sie zu einer höheren Produktion und damit zu einem höheren Wohlstand führt. Dies ist eine Umkehrung von Ursache und Wirkung.

Zeitpräferenz ist das ökonomische Axiom[2], das besagt, dass Menschen ein „gegenwärtiges Gut" einem „zukünftigen Gut" vorziehen. Da diese Idee im Widerspruch zum subjektiven Wert[3] steht, kann sie nicht bewiesen werden. Zeit ist insofern einzigartig, als man davon ausgeht, dass sie einen inhärenten Wert hat. Diese Annahme beruht auf der Beobachtung, dass Menschen nur begrenzt Zeit haben und dass Zeit ein notwendiger Faktor aller Produktion ist.

Der Wert ergibt sich aus der menschlichen Wahrnehmung des Nutzens. Eine Person, die ein Auto gegen ein Pferd eintauscht, schätzt den Nutzen des Besitzes des Pferdes mehr als das Auto. Dies sagt nichts darüber aus, warum das eine für die Person wertvoller ist als das andere, selbst angesichts des Austauschs. Der Wert, der einem Gut gegenüber einem anderen beigemessen wird, ist eine Präferenz[4]. Es kann nicht gezeigt werden, dass eine Person eine Präferenz für ein Gut ausdrücken wird, nicht einmal für ihr eigenes Leben. Der Grund für eine Präferenz ist mit der rationalen Wirtschaftstheorie[5] nicht beweisbar, mit einer Ausnahme – dem Einfluss von Wohlstand auf die Zeitpräferenz.

Abnehmender Grenznutzen[6] impliziert, dass jede zusätzliche Einheit eines Gutes, die eine Person anhäuft, für sie einen geringeren Nutzen hat als die vorherige. Das bedeutet,

Referenzen

[1] https://de.wikipedia.org/wiki/Zeitpräferenz_(Volkswirtschaft)
[2] https://de.wikipedia.org/wiki/Axiom
[3] https://en.wikipedia.org/wiki/Subjective_theory_of_value
[4] https://de.wikipedia.org/wiki/Präferenz_(Wirtschaftswissenschaften)
[5] https://de.wikipedia.org/wiki/Katallaktik
[6] https://de.wikipedia.org/wiki/Grenznutzen

dass bei einem gegebenen Zinssatz steigender Wohlstand eine steigende Bereitschaft zur Kreditvergabe mit sich bringt. Dies ist Ausdruck sinkender Zeitpräferenz und spiegelt sich anschließend in einem sinkenden Zinssatz aufgrund des steigenden Kapitalangebots wider, das um Kredite konkurriert.

Der ökonomische Zinssatz ist lediglich eine Widerspiegelung der Zeitpräferenz. Die Zeitpräferenz einer Person kann durch alles beeinflusst werden, aber nur eine Vermögensänderung impliziert eine notwendige Veränderung. Ein höherer Zinssatz bedeutet, dass eine Person mit einer bestimmten Zeitpräferenz eher bereit ist, Kredite zu vergeben. Es wäre jedoch ein Fehler anzunehmen, dass höhere Zinssätze die Zeitpräferenz erhöhen. Ein ähnlicher Fehler ist die Annahme, dass eine Person wohlhabender wird, wenn sie ihre Zeitpräferenz senkt. Dies sind beides Umkehrungen von Ursache und Wirkung. Daher ist die Theorie ungültig.

Unendliche Zeitpräferenz bedeutet keine Kreditvergabe und daher keine Produktion. Null Zeitpräferenz bedeutet keinen Konsum der produzierten Produkte. Da die Produktion nur zur Befriedigung des späteren Konsums dient, bedeutet null Zeitpräferenz auch keine Produktion, da dem Konsum von Produkten kein Wert zugeschrieben werden kann. Deshalb ist die niedrigste Zeitpräferenz nicht automatisch produktiver. Daher ist die Theorie ungültig. Zeitpräferenz ist ein Gleichgewicht zwischen Konsum und Produktion.

Der Wohlstand eines Menschen steigt nur in dem Maße, in dem er seine Präferenzen befriedigen kann, einschließlich der Präferenzen für gegenwärtigen und aufgeschobenen Konsum. Staaten versuchen mit fiskalischen und monetären Stimuli[1], den Konsum bzw. die Produktion zu steigern. Dies geschieht jedoch auf Kosten der Besteuerung. Das Ergebnis ist die Verlagerung von Kapitalallokationsentscheidungen vom Markt auf den Staat, was dazu führt, dass Kapital für nicht verbrauchte

Referenzen

[1] https://en.wikipedia.org/wiki/Stimulus_(economics)

(Überangebot) oder nicht verfügbare (Knappheit) Produkte verschwendet wird. Dies bedeutet, dass die Menschen ihre Präferenzen weniger *befriedigen* können. An ihren Präferenzen ändert sich jedoch nichts, außer wenn ihr Vermögen durch Steuern verringert oder durch Subventionen erhöht wird.

Die Wirtschaftswissenschaften treffen keine Werturteile, sie schließen auf deren notwendige Konsequenzen. Die Theorie setzt eine Moral voraus, die zwar angenommen werden kann, aber objektiv sein muss. Aggression unterscheidet den freien Markt von Marktinterventionen, etwa durch den Staat. Doch selbst wenn man das Nichtagressionsprinzip[1] als moralische Trennlinie akzeptiert, gibt es keinen moralischen Unterschied zwischen höherer und niedrigerer Zeitpräferenz. Es gibt kein Verhältnis von Konsum zu Produktion, das Aggression impliziert. Es bleibt subjektiv, auch wenn es vom Wohlstand beeinflusst wird. Daher ist die Theorie ungültig.

Es kann aufschlussreich sein, die Subjektivität von Wert im Hinblick auf die sexuelle Präferenz zu betrachten.

```
{ X, Y }
{ X->X, Y->Y }
{ X->X|Y, Y->X|Y }
{ X->Y, Y->X }
```

Man könnte diese Liste als geordnet nach der Steigerung der Produktion (d. h. der Produktion von mehr Menschen) betrachten. Viele Staaten versuchen, das Ausleben sexueller Vorlieben auf die Menge { X->Y, Y->X } zu reduzieren. Zu diesem Zweck werden sowohl die völlige Kriminalisierung[2] der Darstellung als auch explizite finanzielle Anreize[3] verwendet. Dies hat erkennbare Auswirkungen auf das Ausleben sexueller

Referenzen

[1] https://de.wikipedia.org/wiki/Nichtaggressionsprinzip

[2] https://de.wikipedia.org/wiki/Gesetze_zur_Homosexualität

[3] https://en.wikipedia.org/wiki/Marriage_promotion

Vorlieben, aber man kann nicht behaupten, dass es Auswirkungen auf die Vorlieben selbst hat.

Ebenso sollte klar sein, dass eine Produktionssteigerung nicht objektiv gut ist. Menschen tun, was sie bevorzugen, und das ist moralisch gut, wobei wir wiederum das moralische Prinzip der Nichtaggression voraussetzen. Selbst wenn wir annehmen, dass alle Menschen den Fortbestand der Art[1] bevorzugen, hat dies keine Auswirkungen auf die individuellen sexuellen Vorlieben.

Eine verwandte Theorie besagt, dass Menschen eine geringere Zeitpräferenz zur Schau stellen können, indem sie mehr Bitcoin horten. Ein erhöhtes Horten auf Kosten der Kreditvergabe impliziert eine *höhere* Zeitpräferenz. Ein erhöhtes Horten auf Kosten des Konsums scheint eine geringere Zeitpräferenz zu implizieren, da der Konsum aufgeschoben erscheint. Ein Hort stellt jedoch nur die für den Konsum erforderliche Liquidität dar.

Wie beim Glücksspiel[2] ist jede Spekulation Konsum der Kosten für das „Spielen", unterstützt durch die dafür erforderliche Liquidität. Diese Kosten sind mindestens die Opportunitätskosten[3], die entstehen, wenn der Betrag nicht verliehen wird (also die Zinsen). Trotz der Tatsache, dass das Spiel, wie jeder Konsum, Zeit erfordert, wird hier die Präferenz zum Ausdruck gebracht, das Spiel zu spielen und nicht, Zeitwert zu gewinnen. Daher ist auch diese Theorie ungültig.

Es gibt eine damit verbundene Theorie, dass sich Zeitpräferenz durch aufgeschobenen Konsum ausdrückt – wenn also eine Person Ersparnisse anhäuft, anstatt diese

Referenzen

[1] https://futurism.com/in-order-to-ensure-human-survival-we-must-become-a-multi-planetary-species

[2] https://en.wikipedia.org/wiki/Game_of_chance

[3] https://en.m.wikipedia.org/wiki/Opportunity_cost

Ersparnisse zu verbrauchen. Wie in Spekulativer Konsum[1] gezeigt, werden dadurch alle Ersparnisse fälschlicherweise als implizite Investitionen dargestellt. Ersparnisse sind ein allgemeiner Begriff, der sowohl den Hort als auch die Investition einer Person umfasst.

Ersparnisse sind die *Quelle* aller Investitionen, aber nur tatsächliche Investitionen drücken eine Zeitpräferenz aus. Ein Hort kann sich sicherlich in seinem Marktwert ändern. **Aber wenn man einen größeren Hort als Ausdruck einer geringeren Zeitpräferenz betrachtet, ist dies eine häufige umgangssprachliche Fehlinterpretation der wirtschaftlichen Bedeutung des Begriffs.** Dies kehrt die Bedeutung um und führt zu Schlussfolgerungen wie der, dass das Horten des gesamten Kapitals eine Zeitpräferenz von null ausdrückt. Doch bei vollständiger Hortung sind die Zinssätze unendlich, und unendliche Zinsen spiegeln eine unendliche Zeitpräferenz wider. Dieser direkte Widerspruch offenbart die Tatsache, dass die Bedeutung des Begriffs Zeitpräferenz umgekehrt wurde, was die Theorie ungültig macht.

Referenzen

[1] Kapitel: Spekulativer Konsum

GELD

Tautologie des Sammlerstücks

Beim Versuch, das Regressionstheorem[1] auf Bitcoin anzuwenden, könnte man postulieren, dass Bitcoin als „Sammlerstück“ begann, das aus dem Interesse von Geldtheoretikern entstand. Das Sammlerstück erhielt aufgrund ihrer persönlichen Vorlieben einen ursprünglichen Gebrauchswert[2]. Es wurde dann aufgrund dieses Wertes getauscht[3]und entwickelte sich zu einem Tauschmittel[4], basierend auf den erinnerten Tauschwert.

Dies scheint mit dem Theorem[5] übereinzustimmen, das besagt, dass alles Geld[6] aus einer Ware[7] stammen *muss*, welcher zunächst ein Tauschwert und danach ein monetärer Wechselkurs zugeschrieben wird. Wenn ein Warenwert allerdings daraus entstehen kann, dass etwas das Potential hat, Geld zu sein, dann ist das Theorem tautologisch[8], impliziert es doch nicht mehr, als dass Geld Geld ist.

> Ziel des Regressionstheorems ist es nun, die erstmalige Entstehung einer monetären Nachfrage nach einem Gut, das bislang ausschließlich zu industriellen Zwecken nachgefragt wurde, unter dem Einfluss des Tauschwerts zu interpretieren, der ihm in diesem Moment ausschließlich aufgrund seiner nicht-monetären Leistungen zugeschrieben wird.
>
> *Ludwig von Mises: Menschliches Handeln*

Referenzen

[1] Kapitel: Regressionsfehlschluss

[2] https://en.m.wikipedia.org/wiki/Use_value

[3] https://en.m.wikipedia.org/wiki/Barter

[4] https://en.m.wikipedia.org/wiki/Medium_of_exchange

[5] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/4-determination-purchasing-power-money

[6] Kapitel: Taxonomie des Geldes

[7] https://de.wikipedia.org/wiki/Handelsware

[8] https://de.wikipedia.org/wiki/Tautologie_(Logik)

Das Postulat nutzt die umgangssprachliche Mehrdeutigkeit des Wortes „Rohstoff“ aus, trotz des expliziten Verweises auf den „industriellen“ Gebrauchswert im Theorem selbst. **Wenn alles ein Rohstoff sein kann, dann würde das Regressionstheorem entgegen seiner Behauptung implizieren, dass alles Geld sein kann.**

> In der Wirtschaft ist eine Ware ein Wirtschaftsgut oder eine Dienstleistung, die vollständig oder weitgehend fungibel ist: Das heißt, der Markt behandelt Exemplare des Gutes als gleichwertig oder nahezu gleichwertig, ohne Rücksicht darauf, wer sie hergestellt hat. [...]
>
> Die meisten Waren sind Rohmaterialien, Grundressourcen, landwirtschaftliche oder Bergbauprodukte wie Eisenerz, Zucker oder Getreide wie Reis und Weizen. Waren können auch massenproduzierte, nicht spezialisierte Produkte wie Chemikalien und Computerspeicher sein.
>
> *Wikipedia: Commodity*

Das Regressionstheorem verwendet den Begriff „Ware“, um Geld von etwas ohne ursprünglichen Gebrauchswert zu unterscheiden. Wenn er beabsichtigt, dass *irgendetwas* eine Ware ist, ist er tautologisch, und andernfalls ist das Postulat eine falsche Darstellung des Satzes.

Fehlschluss der Schuldenschleife

Es gibt eine Theorie, dass es in modernen staatlichen Währungssystemen[1] kein echtes Geld[2] gibt. Stattdessen sei das, was allgemein als „Fiatgeld" bezeichnet wird, eigentlich ein Geldersatz[3] (z.B. ein rechtlich durchsetzbarer Anspruch auf Geld). Ein Geldersatz ist eine Verpflichtung, den Ersatz für das geliehene Geld einzulösen, das er repräsentiert. Dies stellt also schon per Definition ein Problem dar – die Grundlage des Begriffs „Schleife". Die Theorie beruht auf der Beobachtung, dass der Staat die Währung sowohl ausgibt als auch akzeptiert, was eine Verpflichtung dazu impliziert, wie etwa beim Erlass von Schulden gegenüber dem Staat (z. B. Steuern). Bei der Ausgabe ist der Anspruch also eine Gutschrift auf zukünftige Steuerzahlungen usw. (d. h. das eigentliche Geld).

Allerdings sind Geldersatzmittel Ansprüche auf einen bestimmten Geldbetrag[4], da sie ansonsten nicht fungibel wären. Die Höhe der Steuerschuld, die ein 100-Dollar-Schein als Zahlung von 100 Dollar Steuern darstellt, ist durch sich selbst definiert (d. h. der logische Fehler des Zirkelschlusses[5]). Der Betrag, den sie kompensieren, ist der, den der Staat bereit ist, dafür zu tauschen. Dies wäre für jede Art von Geld der Fall, auch für 100 Unzen Gold oder 100 Einheiten Fiatgeldes. **Geld repräsentiert nicht die Menge eines anderen Gutes, sondern alles, wofür auch immer es getauscht werden kann.**

Der Staat macht keine Schulden, wenn er erklärt, dass er ein Geld akzeptiert, sei es Gold oder Fiatgeld. Ebenso macht ein Unternehmen, das erklärt, dass es ein bestimmtes Geld annimmt, dadurch keine Schulden. Die Schuld bei repräsentativem Geld[6] (einer Form

Referenzen

[1] https://en.wikipedia.org/wiki/Currency

[2] Kapitel: Taxonomie des Geldes

[3] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[4] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[5] https://de.wikipedia.org/wiki/Zirkelschluss

[6] https://en.wikipedia.org/wiki/Representative_money

von Geldersatz) wie etwa einem Goldzertifikat[1], drückt sich im Handel des Goldes gegen die Forderung des Zertifikatsinhabers darauf aus. Die Emission des Geldes ändert nichts an dieser Tatsache. Der Staat oder ein Unternehmen können sicherlich Gold im Handel emittieren, ohne dass das Gold als Schuld gilt. Staatliches Fiatgeld genießt einen Monopolschutz[2] bei der Emission, was dem Staat einen Profit[3] garantiert. Für die Frage, ob es sich bei dem Fiatgeld um Geld oder um Schulden handelt, ist dies jedoch nicht relevant.

Kein Geld hat einen inneren Wert. Fiatgeld unterscheidet sich von Warengeld wie Gold nur durch die Annahme, dass es keinen Gebrauchswert[4] hat. Aber da Wert subjektiv ist[5], ist das kein materieller Unterschied. Und es ist auch kein tatsächlicher Unterschied, da Papiergeld zum Heizen verwendet werden kann. Wenn der Staat Gold oder Bitcoin minen, prägen und akzeptieren würde, müsste die Theorie Goldeinheiten und Bitcoin-Schulden nach denselben Kriterien betrachten wie Fiatgeld.

Die Theorie stellt ein Missverständnis der Natur von Geldersatz dar. Eine Forderung kann keine Forderung für sich selbst sein. In einem solchen Szenario würde sich die Forderung von selbst begleichen[6]. Mit anderen Worten, wenn 100 Dollar eine Forderung für irgendetwas im Wert von 100 Dollar wären, dann wäre das Halten der Forderung die Befriedigung der Forderung. Es wäre überhaupt keine Forderung, sondern Geld. Daher ist die Theorie ungültig.

Der Übergang von einem Anspruch hin zu Fiatgeld findet statt, wenn repräsentatives Geld von seinem Emittenten abgeschafft wird. Der US-Dollar wurde 1934

Referenzen

[1] https://en.wikipedia.org/wiki/Gold_certificate
[2] https://en.wikipedia.org/wiki/Counterfeit
[3] https://en.wikipedia.org/wiki/Seigniorage
[4] https://de.wikipedia.org/wiki/Gebrauchswert
[5] https://en.wikipedia.org/wiki/Subjective_theory_of_value
[6] https://de.wikipedia.org/wiki/Clearing

monetarisiert[1], als seine Einlösbarkeit aufgehoben wurde. Die Menschen waren gezwungen, einlösbare Dollar gegen nicht einlösbare Dollar einzutauschen. Sofern ehemals einlösbare Dollar im Umlauf bleiben, was bei vielen noch der Fall ist, werden sie umgetauscht, wenn sie der Federal Reserve[2] begegnen. Die Beibehaltung der Bezeichnung „Federal Reserve Note“ auf dem nicht einlösbaren Dollar ist anachronistisch.

Jedes Geld impliziert Geldsurrogate als Folge der Kreditvergabe[3]. Wir können vier hypothetische Szenarien für Geldersatzstoffe in Bezug auf die Schuldenregression klassifizieren, wobei jeder Schritt in der Regression ein Schuldschein[4] ist.

- Keine Regression (Geld)
- Einfache Regression (repräsentatives Geld)
- Endliche Regression (Geldersatz)
- Unendliche Regression (unmögliches Geld)

Eine Banknote kann eine Forderung auf eine andere Art von Forderung sein, aber nicht auf sich selbst (d. h. auf das, wofür sie eingetauscht werden kann). Andernfalls gibt es keine tatsächliche Regression und die vermeintliche Forderung *ist* Geld. Dies gilt in dem Fall, in dem die Forderung direkt oder indirekt vollständig zirkulär ist, wie der Begriff „Schleife“ andeutet, da die Banknote sich selbst begleicht. Der Begriff „Schuldenschleife“ ist also einfach eine andere Beschreibung für „Geld“. Beispiele sind Gold, Bitcoin und der uneinlösbare (moderne) US-Dollar.

Referenzen

[1] https://en.wikipedia.org/wiki/Gold_Reserve_Act

[2] https://de.wikipedia.org/wiki/Federal_Reserve_System

[3] Kapitel: Fehlschluss der Kreditausweitung

[4] https://en.wikipedia.org/wiki/Promissory_note

Ein direkter Anspruch (einfache Regression) auf Geld ist repräsentatives Geld, obwohl dieser Begriff im Allgemeinen einer greifbaren Banknote vorbehalten ist, die Warengeld[1] darstellt. Die Banknote stellt Geld direkt dar. Der einlösbare US-Dollar war repräsentatives Geld.

Eine indirekte Forderung stellt eine endliche Abfolge von Forderungen gegenüber anderen dar. Wenn alle Forderungen beglichen sind, ist das Geld im Besitz seines rechtmäßigen Eigentümers, alle Forderungen sind beglichen und alle zirkulären Forderungen sind vollständig saldiert[2]. Beachten Sie, dass bei vollständig zirkulären Forderungen nichts zu begleichen ist (d. h. die Forderung ist Geld).

Eine unendliche Regression von Forderungen kann nicht existieren[3]. Betrachten wir eine hypothetische Banknote, emittiert durch die Staatskasse, einlösbar im Sinne der Kompensation staatlicher steuerlicher Verpflichtungen.

- 1 $ begleicht die Steuerschuld für ein Einkommen von 10 $.
- 10 $ begleichen die Steuerschuld für ein Einkommen von 100 $.
- 100 $ begleichen die Steuerschuld für ein Einkommen von 1000 $.
- und so weiter…

Obwohl die Banknote sich selbst nicht repräsentiert, ist ihre Regression unendlich. Ein Anspruch kann nur gegen eine endliche Anzahl anderer Ansprüche geltend gemacht werden. In diesem Fall ist ein solches Instrument eigentlich keine Banknote und kann nur als Geld gehandelt werden.

Referenzen

[1] https://en.wikipedia.org/wiki/Commodity_money

[2] https://en.wikipedia.org/wiki/Set-off_(law)#Close_out_netting

[3] https://en.wikipedia.org/wiki/Turtles_all_the_way_down

Fehlschluss des idealen Geldes

Es wurde vorgeschlagen[1], dass die Existenz eines internationalen, unpolitischen (d.h. objektiven) „Wertindex“ dazu führen wird, dass die Menschen die Staaten dazu zwingen werden, ihre Währungen „am Index auszurichten“ und so die Preisinflation[2] zu beseitigen. Es wurde auch vorgeschlagen, dass Bitcoin ein solcher Index ist und dieses Szenario herbeiführen wird.

Die vorgesehene Hebelwirkung ist die Möglichkeit, bestimmte staatliche Gelder anderen zu bevorzugen. Die Bewegung erfolgt von Geldern mit höherer Inflation zu Geldern mit niedrigerer Inflation, basierend auf dem Vergleich mit dem Index. Die Konsequenz ist, dass die Staaten ihre individuellen Preisinflationsraten zunehmend am Index ausrichten müssen. Dies führt dazu, dass sich staatliche Gelder „asymptotisch“ dem Zustand des durch den Index dargestellten idealen Geldes[3] annähern.

Ideales Geld ist staatliches Geld mit einer Inflationsrate von null:

> ...es gibt keine ideale Inflationsrate, die als Ziel ausgewählt und gewählt werden sollte, sondern das ideale Konzept wäre notwendigerweise eine Nullrate für das, was man Inflation nennt.
>
> *John F. Nash Jr.: Ideales Geld und asymptotisch ideales Geld*

Der Ausdruck der Theorie ist sowohl vielfältig als auch begrenzt (der Beweis bleibt dem Leser überlassen). Die obige Zusammenfassung drückt jedoch alle wesentlichen Elemente aus. Angesichts dieser Einschränkungen kann es hilfreich sein, mit großzügigen Annahmen zu beginnen. Nehmen wir an, dass eine Währung einen

Referenzen

[1] https://fermatslibrary.com/s/ideal-money-and-asymptotically-ideal-money

[2] https://en.wikipedia.org/wiki/Inflation

[3] https://de.wikipedia.org/wiki/John_Forbes_Nash_Jr.

objektiven Wert ausdrücken kann (siehe Theorie des subjektiven Wertes[1]), dass Bitcoin eine solche Währung ist und dass die Menschen im Allgemeinen in der Lage sind, den Wert von Bitcoin mit anderen wichtigen staatlichen Währungen zu vergleichen. Nehmen wir außerdem an, dass die Menschen trotz des offensichtlichen Widerspruchs im Allgemeinen Bitcoin im Handel verwenden (die Quelle des Index) *und* die Verwendung staatlicher Währungen bevorzugen (eine notwendige Prämisse).

Wenn wir außerdem davon ausgehen, dass die Menschen nicht an gesetzliche Zahlungsmittel[2] gebunden sind und ihre Verwendung konkurrierender Währungen Staaten dazu zwingt, Bitcoin als „Preisziel" zu verwenden, wird die Seigniorage[3] eliminiert. Wie jedoch in der Stabilitätseigenschaft[4] gezeigt, besteht der Zweck von Staatsgeld (Fiatgeld[5]) darin, Seigniorage zu erheben, was eine Steuer ist. Mit anderen Worten, ideales Geld ist ein Steuererhebungssystem, das keine Steuern erhebt. Unter den oben genannten Annahmen ist ideales Geld die Obsoleszenz von Staatsgeld. **Der Vorschlag berücksichtigt nicht den Grund, warum Fiatgeld überhaupt existiert.**

Betrachten wir nun die Annahmen noch einmal. Fiatgeld erfordert die Existenz gesetzlicher Zahlungsmittelgesetze und daher wird Fiatgeld generell vom Greshamschen Gesetz[6] (erstmals verfasst von Nikolaus von Oresme[7] in *De origine, natura, jure et mutationibus monetarum*, ca. 1360) gesteuert:

Referenzen

[1] https://en.wikipedia.org/wiki/Subjective_theory_of_value
[2] https://de.wikipedia.org/wiki/Zahlungsmittel
[3] https://de.wikipedia.org/wiki/Seigniorage
[4] Kapitel: Stabilitätseigenschaft
[5] https://de.wikipedia.org/wiki/Fiatgeld
[6] https://de.wikipedia.org/wiki/Greshamsches_Gesetz
[7] https://de.wikipedia.org/wiki/Nikolaus_von_Oresme

> Diese Beispiele zeigen, dass Greshams Gesetz in Ermangelung wirksamer gesetzlicher Zahlungsmittelgesetze umgekehrt funktioniert. Wenn die Menschen die Wahl haben, welches Geld sie annehmen, werden sie mit Geld handeln, von dem sie glauben, dass es langfristig den höchsten Wert hat. Wenn sie jedoch nicht die Wahl haben und gezwungen sind, jedes Geld anzunehmen, ob gut oder schlecht, werden sie dazu neigen, das Geld mit dem höheren wahrgenommenen Wert in ihrem Besitz zu behalten und das schlechte Geld an jemand anderen weiterzugeben. Kurz gesagt, in Ermangelung gesetzlicher Zahlungsmittelgesetze wird der Verkäufer nichts anderes als Geld eines bestimmten Wertes (gutes Geld) akzeptieren, während die Existenz gesetzlicher Zahlungsmittelgesetze den Käufer dazu veranlassen wird, nur Geld mit dem niedrigsten Warenwert (schlechtes Geld) anzubieten, da der Gläubiger dieses Geld zum Nennwert akzeptieren muss.
>
> *Wikipedia: Greshamsches Gestz*

Der Vorschlag geht fälschlicherweise davon aus, dass das Thiers´sche Gesetz[1] gilt. Wäre dies der Fall, würden die Menschen kein Fiatgeld verwenden. Er ignoriert auch die Existenz von Devisenverkehrsbeschränkungen[2], die speziell dazu dienen, Kapitalflucht[3] zu verhindern. Solche Kontrollen werden mit zunehmender Kapitalflucht verstärkt, um Steuereinnahmen zu sichern. Schließlich schränken solche Kontrollen die Preisfindung im Index erheblich ein, was ihn weniger nützlich macht als die vorgesehene Referenz.

Der Vorschlag bietet keine rationale Erklärung dafür, wie die Menschen angesichts solcher Kontrollen in der Lage sein werden, zwischen staatlichen Geldern hin- und herzuwechseln. Er geht davon aus, dass die Menschen die Steuer aufgrund des Index und ihrer Fähigkeit Vergleiche mit ihm zu ziehen besser erkennen und daher die Steuergier des Staates besser kontrollieren können. Angesichts der nahezu universellen Verwendung von Gold als vergleichsweise objektivem Index vor der Entwicklung des globalen Fiatgeldes ist nicht klar, wie sich Fiatgeld überhaupt durchsetzen konnte, wenn wir davon ausgehen können, dass die Menschen auf diese Weise darauf reagieren werden.

Referenzen

[1] https://de.wikipedia.org/wiki/Greshamsches_Gesetz#Umkehrung

[2] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

[3] https://de.wikipedia.org/wiki/Kapitalflucht

Es gibt das Argument, dass Bitcoin ein objektiver Index ist, Gold hingegen nicht. Dies basiert auf dem inflationären Angebot von Gold im Gegensatz zum festen Angebot von Bitcoin. Dabei wird davon ausgegangen, dass Geldinflation ein instabiles Geld bedeutet, während ein festes Angebot ein stabiles Geld impliziert. Wie in der Stabilitätseigenschaft gezeigt, sind beide Gelder stabil. Das Argument lässt außer Acht, dass der Wert, wie er durch den Index angezeigt wird, eine Folge von Angebot und Nachfrage ist. Die Goldnachfrage wird durch die Inflation stabilisiert und die Bitcoin-Nachfrage wird durch Gebühren stabilisiert.

Die Theorie ist daher ungültig. Entweder wird Fiatgeld aufhören zu existieren oder es wird Steuern einziehen. Staaten verzichten nur unter extremem Zwang und in solchen Fällen nur kurzzeitig auf diese Steuern. Wenn überhaupt, wird Bitcoin das „ideale Geld“ sein, und es wird nicht frei gegen staatliche Gelder gehandelt werden (sofern diese noch vorhanden sind).

Fehlschluss der Inflation

Die Konsenregeln von Bitcoin erzeugen eine Periode der Geldinflation[1]. Es gibt eine Theorie, dass dies dazu führt, dass das Geld an Kaufkraft[2] verliert. Wie in Inflationsprinzip[3] gezeigt, **führt eine Angebotssteigerung eines Marktgeldes zu keiner Änderung der Kaufkraft.** Die Theorie ist daher ungültig.

Die Tatsache, dass Bitcoin nicht preisinflationär ist, bedeutet, dass die Besitzer das Mining nicht „subventionieren". Das von den Minern konsumierte Kapital ist ihr eigenes (Investition), das geschaffene Geld ist ihr eigenes Produkt und die Kapitalrendite (Zinsen) ist eine Folge der Nachfragesteigerung, die sie allein erzeugen – und gleicht damit die Opportunitätskosten[4] des Einsatzes ihres eigenen Kapitals über die Zeit aus.

Referenzen

[1] https://en.wikipedia.org/wiki/Monetary_inflation

[2] https://de.wikipedia.org/wiki/Kaufkraft_(Konsum)

[3] Kapitel: Inflationsprinzip

[4] https://en.m.wikipedia.org/wiki/Opportunity_cost

Taxonomie des Geldes

Fiatgeld hat keinen Gebrauchswert[1]. Es ist als Geld nur insoweit nützlich, als Menschen bereit sind, damit Tauschhandel zu betreiben. Zu diesen Menschen kann ein ausgebender Staat gehören, was häufig der Fall ist, trotzdem ist das kein Unterscheidungsmerkmal. Der Name leitet sich von der Tatsache ab, dass es per Dekret als Geld existiert[2] ("dixitque Deus fiat lux et facta est lux"). Eine solche Erklärung ist jedoch auch kein Unterscheidungsmerkmal. **Fiat ist einfach Geld ohne Gebrauchswert.** Geld mit Gebrauchswert wird als Warengeld[3] bezeichnet.

Während Wert subjektiv ist[4], was es in der Praxis unmöglich macht den Gebrauchswert zu bestimmen, ist die Klassifizierung selbst klar. Papiergeld kann zum Heizen verbrannt werden, dies wird aber normalerweise nicht als materieller Gebrauchswert betrachtet. Bitcoin kann zum Erzeugen von Zeitstempeln[5] verwendet werden, aber auch das wird üblicherweise nicht als materieller Gebrauchswert angesehen. Gold, Silber, Kupfer und anderen Münzen weist man generell einen materiellen Gebrauchswert zu. Wenn der Nennwert des Geldes unter seinen Warenwert fällt, wird es zu einer Ware[6] und wird eingeschmolzen oder gehortet[7].

Ein Geldersatz[8] ist ein vertraglicher Anspruch[9] auf einen bestimmten Geldbetrag, der auf Wunsch eingelöst werden kann. Als solcher stellt ein Geldersatz ein „zukünftiges Gut"

Referenzen

[1] https://de.wikipedia.org/wiki/Gebrauchswert

[2] https://en.wikipedia.org/wiki/Let_there_be_light#Origin_and_etymology

[3] https://de.wikipedia.org/wiki/Primitivgeld

[4] https://en.wikipedia.org/wiki/Subjective_theory_of_value

[5] https://en.wikipedia.org/wiki/Trusted_timestamping

[6] https://de.wikipedia.org/wiki/Venezolanischer_Bolivar

[7] https://de.wikipedia.org/wiki/Greshamsches_Gesetz

[8] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[9] https://financial-dictionary.thefreedictionary.com/Contractual+Claim

dar, während Geld ein „gegenwärtiges Gut“ ist. Fiatgeld ist kein Geldersatz[1] da es nicht gegen einen bestimmten Geldbetrag eingelöst werden kann, es ist das Geld selbst. Schulden werden häufig vom Kreditgeber als Geldersatz verbrieft[2] und garantiert, was als Banknote[3] bekannt ist. Da Wert subjektiv ist, ist es auch nicht möglich zu unterscheiden, ob eine Person die Einlösung oder den Anspruch selbst schätzt, aber im Allgemeinen wird davon ausgegangen, dass die Einlösung geschätzt wird und nicht das Dokument, auf dem sie steht. Wenn ein Geldersatz aufgehoben wird, aber noch gehandelt wird, ist er zu Fiatgeld geworden[4].

Repräsentatives Geld[5] wird oft fälschlicherweise als gegenwärtiges Gut interpretiert, doch da es einen Anspruch (auf das, was es repräsentiert) darstellt, ist es ein Geldersatz. Der goldgedeckte US-Dollar war ein Geldersatz und der moderne US-Dollar ist Fiatgeld. Kontobasierte US-Dollar sind elektronische Geldersatzmittel[6], ebenso wie alle Bitcoin-Verwahrkonten und der Handel mit unbestätigten Transaktionen. Dabei handelt es sich um Versprechen, in Dollar bzw. Bitcoin einzulösen.

Die Dollar, die man in der Hand halten kann, sind Fiatgeld, ebenso wie die Bitcoins, die man mit seinen privaten Schlüsseln ausgeben kann. Der Begriff „Fiatgeld“ allein unterscheidet also nicht zwischen Dollar und Bitcoin. *Allerdings war diese Unterscheidung vor der Existenz von Bitcoin nie erforderlich.* Marktgeld ohne Gebrauchswert galt als nicht möglich[7]. Es gibt jedoch einen wesentlichen Unterschied zwischen diesen beiden Geldarten, von denen keine einen Gebrauchswert hat. Dies erfordert einen neuen Unterscheidungsbegriff.

Referenzen

[1] Kapitel: Fehlschluss der Schuldenschleife
[2] https://de.wikipedia.org/wiki/Verbriefung
[3] https://de.wikipedia.org/wiki/Banknote
[4] https://en.wikipedia.org/wiki/Gold_certificate
[5] https://en.wikipedia.org/wiki/Representative_money
[6] https://www.investopedia.com/terms/e/electronic-money.asp
[7] Kapitel: Regressionsfehlschluss

Der Dollar (wie alle staatlichen Fiatgelder) unterscheidet sich von Bitcoin dadurch, dass er bei der Produktion auf Monopolschutz[1] angewiesen ist. Es ist dieses Verbot des Marktwettbewerbs, das es dem Staat ermöglicht, das Angebot zu begrenzen und damit Seigniorage[2] zu extrahieren.

> Ein Monopol ist die Gewährung eines Sonderprivilegs durch den Staat, das einen bestimmten Produktionsbereich einer bestimmten Einzelperson oder Gruppe vorbehält.
>
> *Murray Rothbard: Mensch, Wirtschaft und Staat*

Das Monopol auf die Produktion von staatlichem Fiatgeld wird durch ein Gesetz gegen Geldfälschung[3] geschaffen. Eine Einheit dieses Geldes gilt als ungültig, wenn sie nicht durch einen autorisierten Vertreter[4] des Staates produziert wurde. Dies unterscheidet sich von Bitcoin, da es durch Marktwettbewerb erzeugt wird und Fälschung durch Vereinbarungen in einem öffentlichen Kassenbuch ausgeschlossen ist. Geld, das durch Gesetz gegen Fälschung gesichert ist, kann dann vernünftigerweise als „Monopolgeld" (nicht zu verwechseln mit Monopoly-Geld[5]) und Bitcoin als „Marktgeld" bezeichnet werden. Wenn der Nennwert von Fiatgeld auf seine Produktionskosten reduziert wird, ist es zu Markgeld[6] geworden.

Warengeld ist auch Marktgeld, da es nicht auf Monopolprivilegien angewiesen ist, um sein Angebot einzuschränken. Wenn das Warengeldangebot zu groß ist, ist es aufgrund der fehlenden Portabilität kein nützliches Geld mehr. Die Unterscheidung zwischen Warengeld und Bitcoin ergibt sich aus kryptodynamischen Prinzipien[7]. Das

Referenzen

[1] https://mises.org/online-book/man-economy-and-state-power-and-market/3-illusion-monopoly-price/definitions-monopoly

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] https://de.wikipedia.org/wiki/Falschgeld

[4] https://www.moneyfactory.gov

[5] https://monopoly.fandom.com/wiki/Monopoly_Money

[6] https://de.wikipedia.org/wiki/Simbabwe-Dollar

[7] Kapitel: Kryptodynamische Prinzipien

Warengeldangebot wird durch den Marktwettbewerb um seine Bereitstellung kontrolliert, als Folge der Marktnachfrage. Es ist kein Fiatgeld aufgrund seines mutmaßlichen Gebrauchswertes.

Sowohl Geld als auch Geldersatzmittel bilden die Währung[1]. Geld wird manchmal als Basisgeld bezeichnet. Alle Geldarten unterliegen der Kreditvergabe und daher notwendigerweise der Kreditausweitung[2] (d. h. in Geldersatzstoffe) und der entsprechenden anteiligen Reservierung[3].

Referenzen

[1] https://de.wikipedia.org/wiki/Währung

[2] Kapitel: Fehlschluss der Kreditausweitung

[3] Kapitel: Definition der Reserve

Die folgende Tabelle bietet Beispiele für jede der oben genannten Klassifizierungen.

- Währung
    - Geld [*Gegenwart*]
        - Warengeld [*Nutzwert*]

            Monopol

            US-Dollar-Münze

            Markt

            Goldbarren
        - Fiatgeld [*kein Nutzwert*]

            Monopol

            US-Dollar-Note

            Markt

            Bitcoin
    - Geldersatz [*Zukunft*]
        - Elektronisch [*immateriell*]

            Konto

            Visa
        - Repräsentativ [*materiell*]

            Banknote

            US-Silberzertifikat

Regressionsfehlschluss

Das Regressionstheorem[1] basiert auf der Annahme, dass die ersten Menschen, die etwas als Geld[2] bewerten, dies aufgrund einer Erinnerung an dessen früheren Gebrauchswert[3] tun müssen, wodurch die Sache schließlich einen Nutzen im Tauschhandel[4] und abschließend einen monetären Wert[5] erhält.

> Kein Gut kann als Tauschmittel eingesetzt werden, das zu Beginn seiner Verwendung zu diesem Zweck nicht aufgrund anderer Verwendungen einen Tauschwert hatte.
>
> *Ludwig von Mises: Menschliches Handeln*

Beachten Sie, dass die Theorie nicht nur versucht, den Ursprung des Geldkonzepts zu erklären, sondern den *von allem, was Geld sein kann*. Mit anderen Worten, wenn ein Gut dieser Entwicklung nicht folgt, ist es kein Geld.

Das Theorem widerspricht der Theorie des subjektiven Wertes[6], auf die es aufbaut. Wert ist subjektiv, was impliziert, dass er auf allem basieren kann, auch wenn diese Grundlage objektiv irrational erscheint.

Der Satz kann seine Regression nicht beenden, da er nicht erklärt, wie eine Person dazu kommt, etwas aufgrund seines ursprünglichen Nutzens zu schätzen. Man muss davon ausgehen (nicht sich erinnern), dass etwas nützlich sein wird, wenn niemand jemals versucht hat, es zu verwenden. Diese Annahme des Nutzens ist die erste Bewertung, die

Referenzen

[1] https://en.wikipedia.org/wiki/Regression_theorem

[2] Kapitel: Taxonomie des Geldes

[3] https://de.wikipedia.org/wiki/Gebrauchswert

[4] https://de.wikipedia.org/wiki/Tauschhandel

[5] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/4-determination-purchasing-power-money

[6] https://en.m.wikipedia.org/wiki/Subjective_theory_of_value

subjektiv bleibt. Die erste Bewertung einer Sache kann, wie alles andere auch, aus jedem beliebigen Grund erfolgen, einschließlich ihrer Verwendung als Geld[1].

Es wurde vorgeschlagen[2], dass bei einem bereits bestehenden Konzept von Geld die Erwartung, Geld zu sein, ausreicht, um das Theorem zu erfüllen. Mit anderen Worten, das Geld muss in der Praxis nicht der Entwicklung folgen. In diesem Fall kann bei einem bereits bestehenden Konzept von Geld alles als Geld beginnen. Diese Interpretation macht den Satz tautologisch – alles, was die Menschen als Geld wertschätzen, kann Geld sein. Mit anderen Worten, er reduziert sich auf den subjektiven Erstwert.

Das Theorem basiert tatsächlich auf der *empirischen* Beobachtung der monetären Entwicklung. Doch die rationale Wirtschaftstheorie[3], auf der es basiert, und das Theorem selbst lehnen den Empirismus ausdrücklich ab.

> Alle diese im Regressionstheorem enthaltenen Aussagen werden apodiktisch ausgesprochen, wie es der Apriorismus der Praxeologie impliziert. Es muss so geschehen. Niemandem kann es jemals gelingen, einen hypothetischen Fall zu konstruieren, in dem die Dinge anders geschehen würden.

Eines der vielen Probleme der empirischen Ökonomie ist, dass neue Beobachtungen frühere Schlussfolgerungen widerlegen können. Bitcoin hat dies mit diesem Theorem getan, das angeblich nicht empirisch ist. Es lässt sich deutlich erkennen, dass Satoshi beabsichtigte ein Geld zu schaffen[4], das von vornherein als Geld genutzt werden sollte.

Die Idee ist eine vernünftige empirische *Theorie* über die Entwicklung des Geldbegriffs, aber ungültig als rationales *Theorem* zur Unterscheidung von Geld und Nicht-Geld. Geld wird durch bestimmte Verhaltensweisen der Menschen unterschieden. Die

Referenzen

[1] Kapitel: Tautologie des Sammlerstücks

[2] https://mises.org/library/cryptocurrencies-and-wider-regression-theorem

[3] https://de.wikipedia.org/wiki/Katallaktik

[4] https://bitcoin.org/bitcoin.pdf

Schlussfolgerung, dass etwas Geld ist, besteht in der Beobachtung dieser Verhaltensweisen, einer streng empirischen Methode.

Definition der Reserve

Die Reserve ist das Kapital, das eine Person besitzt. Es ist das vorhandene Kapital, im Gegensatz zum investierten Kapital. Vorliegendes Kapital entwertet[1] und stellt als solches für den Eigentümer laufende Kosten dar. Das Verhältnis von reserviertem zu investiertem Kapital spiegelt[2] die Zeitpräferenz[3] des Eigentümers wider.

Das zur Tilgung[4] von Schulden bestimmte Reservekapital ist das Tilgungsmedium. Wenn beispielsweise Gold das Tilgungsmedium ist, ist Gold das Reservekapital. Ein Versprechen auf Gold, wie etwa ein Goldzertifikat[5], ist ein Darlehen und daher keine Reserve gegen die Schuld. Wenn die Schuld mit Goldzertifikaten getilgt werden kann, dann stellt der Besitz der Zertifikate eine Reserve dar.

Obwohl es auf den ersten Blick der Definition einer Reserve als Kapitalrücklage zu widersprechen scheint, ein Zertifikat als Rücklage zu halten, ist dies nicht der Fall. Als Zahlungsmittel ist das Zertifikat selbst für den Inhaber nichts weiter als ein Stück Papier. Die damit verbundenen Bedingungen sind an den Emittenten des Zertifikats weiterzugeben. Der Inhaber des Zertifikats erleidet durch die Abwicklung des Zertifikats weder Kosten noch Gewinne. Seine Abwicklungskosten sind lediglich eine Folge der Übertragung des Papiers an seinen Gläubiger.

Reserve wird häufig mit Fälligkeitsanpassung[6] verwechselt. Das Management unterschiedlicher Kreditlaufzeiten[7] und Zinssätze ist eine Risikomanagementstrategie.

Referenzen

[1] Kapitel: Abschreibungsprinzip
[2] Kapitel: Sparverhältnis
[3] Kapitel: Zeitpräferenzfehlschluss
[4] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)
[5] https://en.wikipedia.org/wiki/Gold_as_an_investment#Certificates
[6] https://en.m.wikipedia.org/wiki/Asset-liability_mismatch
[7] https://de.wikipedia.org/wiki/Fälligkeit

Während die Kapitalreservierung auch eine Risikomanagementstrategie ist, **besteht der Unterschied einer Reserve darin, dass reserviertes Kapital „vorhanden“ ist und eine Laufzeit von null hat.**

Fehlschluss des risikofreien Zinssatzes

Das hypothetische Konzept des risikofreien Zinssatzes[1] ist der ökonomische Zinssatz, der mit einer garantierten Rückzahlung der Kreditsumme erzielt werden kann. Es gibt eine Theorie, dass Bitcoin dies in der Praxis ermöglicht, indem es die Rückzahlung des Kapitals erzwingt. Eine Folge der Theorie ist, dass diese Fähigkeit die Kreditausweitung[2] generell begrenzen kann.

Die Theorie erfordert eine nachweisbare, zeitlich befristete Verpflichtung[3] des Kreditgebers hinsichtlich der verliehenen Einheiten des Coins. Die Verpflichtung stellt sicher, dass der Kreditgeber die Einheiten bis zur Fälligkeit[4] des Kredits nicht ausgeben kann und dass das Eigentum an den Einheiten zu diesem Zeitpunkt an den Kreditgeber zurückkehrt. Der Kreditgeber tauscht diese belasteten Einheiten mit einem Kreditnehmer gegen Zinsen. Die Opportunitätskosten[5] des Kreditgebers, die ihm durch die Verpflichtung auferlegt werden, werden durch diese Zinsen ausgeglichen.

Für den Kreditnehmer haben die Einheiten jedoch keinen Geldwert. Die volle Kontrolle über die Einheiten geht nachweislich an den Kreditgeber zurück, sodass jede Person, die sie angenommen hat, zu diesem Zeitpunkt mit leeren Händen dasteht. **Dieser Nullwert wird zwangsläufig jedem Tausch vor Fälligkeit und damit dem Kredit selbst zugerechnet, was die Theorie ungültig macht.**

Es gibt eine verwandte Theorie, dass die Opportunitätskosten des Kreditgebers verwendet werden können, um eine nachweisbare Ausgabe darzustellen, genau wie

Referenzen

[1] https://de.wikipedia.org/wiki/Risikofreier_Zinssatz

[2] Kapitel: Fehlschluss der Kreditausweitung

[3] https://de.wikipedia.org/wiki/Covenant_(England_und_Wales)

[4] https://de.wikipedia.org/wiki/Fälligkeit

[5] https://de.wikipedia.org/wiki/Opportunitätskosten

beim Proof-of-Work. Dies kann ähnlich wie Hashcash[1] verwendet werden, um Denial-of-Service-Angriffe[2] abzuschwächen. Das ist richtig, dennoch ist dies ein Aufwand und kann ebenso durch Ausgabe (einschließlich Zerstörung) von Einheiten erreicht werden. Genau wie beim Proof-of-Work handelt es sich hierbei um einen Tausch von nachweisbaren Kapitalkosten gegen Einheiten. Als solches handelt es sich nicht um ein Darlehen (d. h. es bringt keine Zinsen ein), was die Theorie ungültig macht.

Es gibt eine verwandte Theorie, dass die Einheiten vom Kreditnehmer stattdessen verwendet werden können, um einem Vermögenswert mit zeitlich unbegrenztem Wert zu folgen. Da die Verfolgung bei Fälligkeit erlischt, ist diese Theorie aus demselben Grund ungültig. Es gibt eine weitere verwandte Theorie, dass die verliehenen Einheiten verwendet werden können, um einem Vermögenswert mit fester Laufzeit zu folgen, der bei Fälligkeit des Kredits erlischt (z. B. eine Theaterkarte). Dies ist richtig, jedoch sind die Kosten der Verfolgung für jede Dauer in BTC durch die Dust-Konsensregel auf eine Einheit begrenzt. Daher sind die Opportunitätskosten auf eine Einheit plus mindestens eine Transaktionsgebühr für die Einrichtung des Kredits begrenzt.

Der Nutzen für den Kreditnehmer liegt in der Reduzierung der Tracking-Kosten während der Kreditlaufzeit. Bei einem Zinssatz von 10 % und einer Laufzeit von ungefähr 7,2 Jahren[3] ist es günstiger, eine Einheit auszugeben, als sie zu leihen. Indem man stattdessen nur eine Einheit direkt ausgibt, kann der Vermögenswert dauerhaft abgebildet werden.

Obwohl das letzte Szenario ökonomisch vernünftig ist, kann es nicht direkt als Darlehen bezeichnet werden, da die Einheit vom sogenannten Kreditnehmer weder gehandelt

Referenzen

[1] https://de.wikipedia.org/wiki/Hashcash

[2] https://de.wikipedia.org/wiki/Denial_of_Service

[3] https://de.wikipedia.org/wiki/72er-Regel

noch zerstört werden kann. Es wäre angemessener, dies als „Miete“ der Einheit zu bezeichnen, schon allein, um es von einer echten Kreditvergabe zu unterscheiden.

Dennoch kann theoretisch eine Rendite auf die Miete einer Einheit erzielt werden, bis zu der durch den Zinssatz gesetzten wirtschaftlichen Grenze (z. B. ~7,2 Jahre bei 10 %). Die Gebühr, die erforderlich ist, damit dies wirtschaftlich rational ist, muss jedoch null Einheiten betragen, da die mietbegründende Transaktion erforderlich ist, was bei der Verwendung der eigenen Einheit zur Indexabbildung nicht der Fall ist. In dem Fall, in dem die Transaktionsnachfrage das feste Bestätigungsangebot übersteigt, ist dieses Szenario also nicht wirtschaftlich rational. Diese Beziehung gilt bei jedem erzwungenen Dust-Niveau des Coins über null, sofern der Dust (Staub, Rest) eine unzureichende Gebühr darstellt, um die Bestätigung zu finanzieren.

Aus-dem-Nichts-Fehlschluss

Es gibt eine Theorie, dass das Teilreservebankwesen[1] den Banken von Natura aus die Möglichkeit gibt, Geld ohne materielle Kosten zu erschaffen. Die Theorie hängt nicht vom staatlichen Privileg der Seigniorage[2] ab. Sie wird als Folge der Buchhaltungspraktiken des freien Bankwesens[3] betrachtet. Dies wird manchmal als Geldschöpfung *ex nihilo* oder „aus dem Nichts"[4] bezeichnet.

> Banken nehmen nicht, wie es noch immer in zu vielen Lehrbüchern vorgeschlagen wird, Einlagen von Sparern an und verleihen sie an Kreditnehmer: Sie schaffen Kredit und Geld aus dem Nichts – sie gewähren dem Kreditnehmer einen Kredit und schreiben ihn gleichzeitig seinem Geldkonto gut.
>
> *Lord Turner, Vorsitzender der britischen Finanzaufsichtsbehörde bis zu ihrer Abschaffung im März 2013*
> *Konferenz der Stockholm School of Economics zum Thema: „Auf dem Weg zu einem nachhaltigen Finanzsystem"*
> *12 September 2013*

Anhänger beschreiben zwei konkurrierende Ansichten zur Geldschöpfung. Das traditionelle Verständnis ist im Vergleich zu ihrer praktischeren Sichtweise naiv, wie Lord Turner andeutet. Die Theorie besagt, dass das Bankwesen von Natur aus nicht nur Kredit, sondern auch Geld schafft.

Naive Sichtweise

Geld wird von Minern zu einem materiellen Preis geschaffen, möglicherweise an Menschen verkauft und schließlich an Menschen verliehen. Diese Theorie geht davon aus, dass der Kreditgeber nur Geld verleiht, das er besitzt. Daher arbeitet der Kreditgeber

Referenzen

[1] https://de.wikipedia.org/wiki/Mindestreserve-System

[2] https://de.wikipedia.org/wiki/Seigniorage

[3] https://en.wikipedia.org/wiki/Free_banking

[4] https://cdn.evbuc.com/eventlogos/67785745/turner.pdf

mit voller Reserve[1] und kann nicht die Praxis der Teilreserve anwenden, die als betrügerisch gilt. Als ein ehrlicher Kreditgeber kann er Forderungen (repräsentatives Geld[2]) nur gegen Geld ausstellen, das er besitzt, wodurch Kreditausweitung[3] und damit eine anhaltende Preisinflation[4] verhindert werden.

Praktische Sichtweise

Geldersatzmittel werden von Banken ohne materielle Kosten als Folge der Teilreservekreditvergabe geschaffen. Das Angebot dieser Ersatzmittel wächst mit jedem Kredit und verringert sich nur, wenn Kredite zurückgezahlt[5] werden. Da es keine Beschränkungen für die Kreditausweitung gibt, wächst die Gesamtverschuldung grenzenlos und führt zu einer anhaltenden Preisinflation.

In einem freien Markt können Menschen dieselben Geschäfte tätigen wie Banken, ohne sich notwendigerweise als Banken zu bezeichnen. Daher muss die Unterscheidung zwischen diesen beiden Möglichkeiten auf der Verschleierung des vermeintlichen Betrugs beruhen. Die Theorie besagt, dass diese Verschleierung durch einen Buchhaltungstrick erreicht wird, der nicht allgemein verstanden wird. Lassen Sie uns also den Unterschied untersuchen. Für diese Untersuchung der in beiden Fällen geschaffenen Geldersatzmittel[6] reicht jedes Geld aus, einschließlich Gold, Bitcoin oder Monopolgeld[7].

Referenzen

[1] Kapitel: Vollreservefehlschluss

[2] https://en.wikipedia.org/wiki/Representative_money

[3] Kapitel: Fehlschluss der Kreditausweitung

[4] https://de.wikipedia.org/wiki/Inflation

[5] https://de.wikipedia.org/wiki/Clearing

[6] https://mises.org/online-book/human-action/chapter-xvii-indirect-exchange/11-money-substitutes

[7] Kapitel: Taxonomie des Geldes

In der naiven Sichtweise hat der potenzielle Kreditgeber sowohl die für den persönlichen Konsum erforderliche Liquidität (Hort) als auch den zur Verzinsung vorgesehenen Betrag (Kapitalanlage) gespart. Alle Kredite in diesem Szenario stammen aus Ersparnissen, wie z. B. aus Gold, das er beim Goldwaschen[1] angesammelt hat. Ersparnisse umfassen die Summe des Hortes (Geld) und den Betrag, um den der Kredit die Schulden übersteigt: Ersparnisse = Geld + (Kredit - Schulden). Geld ist Gold und Kredite sind Geldersatz.

	Ersparnisse	Geld	Kredit	Schulden
Person	100oz	100oz		

In dieser Ansicht der Privatkreditvergabe übergibt die Person dem Schuldner 81 Unzen Gold. Der Schuldner verpflichtet sich, der Person das Geld bei Fälligkeit[2] des Kredits samt Zinsen zurückzuzahlen. Zur Vereinfachung der Bilanzierung gehen wir von Nullzinsen und keiner Bilanzierung (d. h. Diskontierung) für das Rückzahlungsrisiko aus:

	Ersparnisse	Geld	Kredit	Schulden
Person	100oz	19oz	81oz	
Schuldner		81oz		81oz

Die Person hat ihrem eigenen Unternehmen (z. B. Kreditgeschäft) tatsächlich einen Bruchteil ihrer Ersparnisse geliehen, der im Folgenden ausgewiesen wird. Nehmen wir an, dass die Person 10 % ihrer Ersparnisse für die für den kurzfristigen Konsum erforderliche Liquidität hortet, und sein Unternehmen 10 % aus demselben Grund:

Referenzen

[1] https://en.m.wikipedia.org/wiki/Gold_panning

[2] https://en.wikipedia.org/wiki/Maturity_(finance)

	Ersparnisse	Geld	Kredit	Schulden
Person	100oz	10oz	90oz	
Unternehmen		9oz	81oz	90oz
Schuldner		81oz		81oz

Das Unternehmen der Person arbeitet mit 10 % Reserve, da 90 % ihres eingezahlten Geldes ausfallgefährdet sind. Um dies in die naive Sichtweise des Bankwesens zu übertragen, muss lediglich „Kreditgeber“ in „Einleger“ und „Unternehmen“ in „Bank“ umbenannt werden. Es besteht keine Notwendigkeit anzunehmen, dass es sich dabei um unterschiedliche Personen handelt:

	Ersparnisse	Geld	Kredit	Schulden
Einleger	100oz	10oz	90oz	
Bank		9oz	81oz	90oz
Schuldner		81oz		81oz

Wenn wir richtigerweise berücksichtigen, dass die Person Geld riskiert (d.h. Einleger ist), können wir sehen, dass alle Kredite nur teilweise reserviert sind. In diesem Szenario gibt es zwei Kredite, die zu 10 % reserviert sind, was zu Geldsubstituten (Krediten) von 171 % des Geldes führt. Unter der Annahme einer einheitlichen Zeitpräferenz[1] wird der Schuldner 90 % seiner Ersparnisse verleihen, ebenso wie alle nachfolgenden Schuldner. Unter der Annahme eines praktischen Mindestkredits von 1 Unze endet die Kreditausweitung nach 43 Krediten bei dem 8,903-fachen des Geldbetrags.

Referenzen

[1] Kapitel: Zeitpräferenzfehlschluss

Dabei ist r die einheitliche Höhe der individuellen Reserven und m die Geldmenge. Die Gesamtkreditsumme c für eine beliebige Anzahl n von Krediten ergibt sich aus der folgenden Teilsumme[1]:

```
c = ∑(n=1..n)[m * (1 - r)^n] =
(m * (r - 1) ((1 - r)^n - 1))/r =
(100oz * (10% - 1) ((1 - 10%)^43 - 1))/10% = 890,3oz
```

Die Reservequote[2] rr ergibt sich aus dem Verhältnis von Geldmenge zu Kredit:

```
rr = m/c = 100oz/890,3oz = ~11,23%
```

Der Geldschöpfungsmultiplikator[3] ergibt sich aus dem Kehrwert der Reservequote:

```
1/rr = 1/(100oz/890,3oz) = 8,903
```

Nur weil ein einzelner Dollar als kleinste verleihbare Einheit gilt, ist die Serie auf 43 Iterationen beschränkt. Eine stetige Funktion ergibt einen Geldschöpfungsmultiplikator von 9 bei 10 % Hortung.

Durch Iteration ergibt sich folgende Tabelle:

Referenzen

[1] https://www.wolframalpha.com/input/?i=sum+of+m+*+(1-r)%5En+as+n+goes+from+1+to+infinity

[2] https://de.wikipedia.org/wiki/Mindestreserve

[3] https://de.wikipedia.org/wiki/Geldschöpfungsmultiplikator

Darlehen	Gehortet	Verliehen	Kredit
1	10,00	90,00	90,00
2	19,00	81,00	171,00
3	27,10	72,90	243,90
4	34,39	65,61	309,51
5	40,95	59,05	368,56
6	46,86	53,14	421,70
7	52,17	47,83	469,53
8	56,95	43,05	512,58
9	61,26	38,74	551,32
10	65,13	34,87	586,19
11	68,62	31,38	617,57
12	71,76	28,24	645,81
13	74,58	25,42	671,23
14	77,12	22,88	694,11
15	79,41	20,59	714,70
16	81,47	18,53	733,23
17	83,32	16,68	749,91
18	84,99	15,01	764,91
19	86,49	13,51	778,42
20	87,84	12,16	790,58

21	89,06	10,94	801,52
22	90,15	9,85	811,37
23	91,14	8,86	820,23
24	92,02	7,98	828,21
25	92,82	7,18	835,39
26	93,54	6,46	841,85
27	94,19	5,81	847,67
28	94,77	5,23	852,90
29	95,29	4,71	857,61
30	95,76	4,24	861,85
31	96,18	3,82	865,66
32	96,57	3,43	869,10
33	96,91	3,09	872,19
34	97,22	2,78	874,97
35	97,50	2,50	877,47
36	97,75	2,25	879,72
37	97,97	2,03	881,75
38	98,18	1,82	883,58
39	98,36	1,64	885,22
40	98,52	1,48	886,70
41	98,67	1,33	888,03

42	98,80	1,20	889,22
43	98,92	1,08	890,30

Man beachte, dass bei voller Expansion, damit irgendeine Person Geld aus ihrem Hort ausgeben und gleichzeitig ihre Zeitpräferenz beibehalten kann, ein Kredit getilgt werden muss, um die Ausgaben auszugleichen. Der Abrechnungsprozess überträgt das Geld vom ehemaligen Kreditnehmer auf den Kreditgeber und storniert den Schuldschein. Die Person, die das ausgegebene Geld erhält, muss es verleihen, um ihre Zeitpräferenz zu erfüllen, und so weiter.

Ohne eine Erhöhung der Geldmenge oder eine allgemeine Verringerung der Zeitpräferenz ist keine weitere Expansion möglich. Eine Erhöhung der Geldmenge erhöht die absolute Kreditmenge und eine Verringerung der Zeitpräferenz erhöht das Verhältnis von Kredit zu Geld. Da sich Geld und Kredit gemeinsam entwickeln, kommt es ohne diese Änderungen nie zu einer tatsächlichen Erhöhung der Geldsubstitute.

In der üblichen Praxis der Bankbuchhaltung übergibt die Bank das Geld nicht. Stattdessen erstellt sie Konteneinträge in einem als „Kreditschaffung“ bezeichneten Prozess. Sie erstellt Gegenbuchungen[1] für die Erlöse und das Darlehen des Einlegers („Kredit“ und „Schulden“) und Gegenbuchungen in der Bilanz[2] für sich selbst („Vermögenswert“ und „Verbindlichkeiten“). Zum Zeitpunkt der Kreditvergabe lauten die Konten wie folgt:

Referenzen

[1] https://de.wikipedia.org/wiki/Kassenbuch

[2] https://de.wikipedia.org/wiki/Bilanz

	Ersparnisse	Geld	Kredit	Schulden	Vermögens-werte	Verbindlich-keiten
Einleger	100oz	10 oz	90oz		100oz	
Bank		90 oz	81oz	171oz	171oz	171oz
Schuldner			81oz	81oz	81oz	81oz

Hier enden die Erklärungen der Theorie[1] meist. Die Gegenkonten von Bank und Kreditnehmer sind ausgeglichen, aber der Kreditnehmer hat 81 Unzen Gold zum Ausgeben, und die Bank musste dem Kreditnehmer kein Gold übergeben. Es sind immer noch nur 100 Unzen Geld vorhanden, aber der Kreditnehmer hat 81 Unzen Geldersatz und die Bank hat 81 Unzen mehr an Vermögenswerten. Die Theorie besagt, dass die Bank somit nicht nur Kredit, sondern auch *Geld* geschaffen hat. Beachten Sie, dass immer noch alles ausbalanciert ist und alle Konten ausgeglichen werden können, was scheinbar die von Lord Turner vertretene Theorie bestätigt, dass „... sie Kredit und Geld aus dem Nichts schaffen – indem sie dem Kreditnehmer einen Kredit gewähren und gleichzeitig dem Geldkonto des Kreditnehmers gutschreiben."

Dies zeigt jedoch, dass weder der Kredit noch das Bankvermögen tatsächlich ausgegeben wurden. Gehen wir noch einen Schritt weiter und gehen wir davon aus, dass der Schuldner sein Konto und damit auch die entsprechenden Vermögens- und Verbindlichkeitseinträge der Bank bereinigt.

Referenzen

[1] https://www.sciencedirect.com/science/article/pii/S1057521915001477

	Ersparnisse	Geld	Kredit	Schulden	Vermögens-werte	Verbindlich-keiten
Einleger	100oz	10oz	90oz		100oz	
Bank		9oz	81oz	90oz	90oz	90oz
Schuldner		81oz		81oz	81oz	81oz

Beachten Sie, dass dies mit dem Ergebnis der naiven Ansicht identisch ist. **Es gibt keinen Unterschied zwischen diesen angeblich konkurrierenden Ansichten zur Geldschöpfung**, was die Theorie ungültig macht. Dies löst die Jahrhunderte alte Debatte[1], die offenbar zwischen Platon[2] und Aristoteles[3] begann und sich darauf bezieht, ob Geld auf Bergbau oder Kredit basiert. Die Theorien sind identisch, da Geld und Kredit eine Dualität[4] darstellen.

> Laut Joseph Schumpeter war Platon der erste bekannte Vertreter einer Kredittheorie des Geldes. Schumpeter beschreibt den Metallismus als die andere von „zwei grundlegenden Geldtheorien" und sagt, der erste bekannte Vertreter des Metallismus sei Aristoteles gewesen.

Die Anhänger der beiden Theorien reden aneinander vorbei[5]. Bitcoin als Fiatgeld (d.h. Geld ohne Gebrauchswert[6]) ohne staatliche Unterstützung[7] hat endlich sowohl die logischen Fehler des Metallismus[8], der die Notwendigkeit eines Gebrauchswertes für

Referenzen

[1] https://en.wikipedia.org/wiki/Credit_theory_of_money#Scholarship

[2] https://de.wikipedia.org/wiki/Platon

[3] https://de.wikipedia.org/wiki/Aristoteles

[4] https://en.wiktionary.org/wiki/duality

[5] https://en.m.wikipedia.org/wiki/Talking_past_each_other

[6] https://de.wikipedia.org/wiki/Gebrauchswert

[7] Kapitel: Wertversprechen

[8] https://de.wikipedia.org/wiki/Metallismus

Geld zu belegen versuchte[1], als auch die des Chartalismus[2], der die Notwendigkeit staatlicher Unterstützung für Fiatgeld zu belegen versuchte[3], sichtbar gemacht.

Denken Sie daran, dass jeder Kredit zu 10 % reserviert ist, sodass die Bank das 8,903-fache des in Reserve befindlichen Geldbetrags verleihen kann, oder 890,3 Unzen Geld als Ersatz für 100 Unzen reserviertes Geld. Wenn die Bank jeden Kredit zu 0 % reserviert, wäre die Kreditausweitung unendlich. Dies impliziert jedoch eine Zeitpräferenz von null oder die Idee, dass Zeit keinen Wert hat, was bedeutet, dass alles Geld auf unbestimmte Zeit verliehen wird. Im Falle einer Bank bedeutet eine Reserve von 0 % keine Liquidität, um Abhebungen auszugleichen (d. h. sofortiger Ausfall). Angesichts einer Zeitpräferenz von null könnte es jedoch niemals Abhebungen geben, was das Szenario irrelevant macht. Die Kreditausweitung ist notwendigerweise endlich.

Betrachten wir also noch einmal das Szenario, in dem eine Bank Kredite mit negativer Reserve (also aus dem Nichts) schafft, diesmal unter Berücksichtigung der Ausgaben. Beispielsweise beabsichtigt die Bank, auf Einlagen von 0 Unzen einen Kredit von 1000 Unzen zu vergeben. Anstatt sich auf reserviertes Geld zu verlassen, um den Kredit schließlich zurückzuzahlen, „schafft" die Bank Geld in ihrer Bilanz. Die Bank erhöht dann die Kredit- und Schuldenkonten des Schuldners, die das geliehene Geld bzw. die Rückzahlungsverpflichtung darstellen:

Referenzen

[1] Kapitel: Regressionsfehlschluss

[2] https://de.wikipedia.org/wiki/Chartalismus

[3] Kapitel: Fehlschluss der Schuldenschleife

	Ersparnisse	Geld	Kredit	Schulden	Vermögens-werte	Verbindlich-keiten
Bank			1000oz	1000oz	1000oz	1000oz
Schuldner			1000oz	1000oz	1000oz	1000oz

Wenn der Schuldner 1 Unze (von seinem Kreditkonto) gegen ein Auto eintauscht, verringert sich sein Kreditkonto um 1 Unze und das des Händlers erhöht sich um 1 Unze. Beachten Sie, dass der Schuldner der Bank nun 1 Unze schuldet, wie im Kreditvertrag vorgesehen.

	Ersparnisse	Geld	Kredit	Schulden	Vermögens-werte	Verbindlich-keiten
Bank			1000oz	1000oz	1000oz	1000oz
Schuldner	-1oz		999oz	1000oz	999oz	1000oz
Händler	1oz		1oz		1oz	

Alles sieht gut aus, bis der Händler versucht, Geld von seinem Konto abzuheben. Zu diesem Zeitpunkt ist die Bank in Verzug und der Händler ist im Rückstand. Wenn das Konto des Händlers bei einer anderen Bank liegt, schlägt die Zahlung fehl, sobald die beiden Banken versuchen, die Konten auszugleichen. Bei einer hypothetischen negativen Reserve ergibt sich folgender Kontostand, was auf eine Bankenpleite[1] (negatives Geld) hindeutet:

Referenzen

[1] https://en.wikipedia.org/wiki/Bank_failure

	Ersparnisse	Geld	Kredit	Schulden	Vermögens-werte	Verbindlich-keiten
Bank	-1oz	-1oz	1000oz	999oz	999oz	999oz
Schuldner			999oz	1000oz	999oz	1000oz
Händler	1oz	1oz			1oz	

Das Geld muss tatsächlich transferiert werden[1], aus der Kontrolle der Bank zum Händler oder zur Bank des Händlers, was nicht möglich ist. Ein einfacheres Beispiel ist der fehlgeschlagene Versuch des Schuldners, Geld von seinem Konto abzuheben[2]. Die Bank kann so viel Geldersatz schaffen, wie sie will, aber eine negative Reserve ist nur ein leeres Versprechen[3]. In diesem Beispiel hat die Bank 1000 Unzen an Versprechen gemacht, die sie nicht einhalten kann.

Das Versäumnis, diese Prinzipien anzuerkennen, resultiert wahrscheinlich aus der mangelnden Berücksichtigung des Abrechnungsprozesses[4]. Dies rührt wahrscheinlich daher, dass die inhärente *Dualität von Geld und Kredit* nicht anerkannt wird, da ersteres immer vorhanden sein muss, um die durch letzteres implizierten Forderungen zu begleichen. Dies rührt wahrscheinlich daher, dass man Geld (z. B. Gold) in den gleichen Begriffen wie Geldersatz (z. B. Kredite für Gold) verwendet.

Die ausgleichenden Aktiva- und Passiva-Einträge dienten nur zur Verrechnung der vergebenen und ausstehenden Kredite, die die Grundlage der Bilanz der Bank bilden. Ebenso wenig hat die Bank die gegenläufigen Kredit- und Schulden-Einträge erstellt, um

Referenzen

[1] https://us.brinks.com/bank-notes

[2] https://de.wikipedia.org/wiki/Geldautomat

[3] https://de.wiktionary.org/wiki/leeres_Versprechen

[4] https://www.youtube.com/watch?v=IzE038REw2k

betrügerische Geldschöpfung zu verschleiern. Die Bank hat diese Konten aus zwei Gründen erstellt:

- Vermeidung physischer Transfers, nur um das Geld wieder bei der Bank einzuzahlen.
- Ermutigung zur erneuten Einzahlung bei der gleichen Bank im Gegensatz zur Konkurrenz (oder dem Hort des Schuldners).

Wenn die Reserven einer Bank nicht ausreichen, um Abhebungen zu ermöglichen, sei es aufgrund von Kreditausfällen oder eines Bankansturms[1], hat sie nur zwei Möglichkeiten: Zahlungsausfall oder Kreditaufnahme. Um Ersteres zu verhindern, gibt es Zentralbanken[2]. Das ist die Bedeutung des Begriffes „Kreditgeber letzter Instanz"[3]. Das Staatsbankenprinzip[4] bietet eine detaillierte Erklärung dieser tatsächlichen Quelle der Geldinflation[5].

Zusammenfassend wurde Folgendes gezeigt:

- Banken sind nicht in der Lage, Geld zu schaffen.
- Teilreserven sind ein fester Bestandteil der Kreditvergabe.
- Der Teilreservebetrag ist Ausdruck der Zeitpräferenz.
- Nullreserven schließen jegliche Möglichkeit aus, Rechnungen begleichen zu können.
- Es besteht kein Unterschied zwischen den naiven und praktischen Theorien der Gelschöpfung.

Referenzen

[1] https://de.wikipedia.org/wiki/Bankansturm
[2] https://de.wikipedia.org/wiki/Zentralbank
[3] https://de.wikipedia.org/wiki/Kreditgeber_letzter_Instanz
[4] Kapitel: Staatsbankenprinzip
[5] https://en.wikipedia.org/wiki/Monetary_inflation

Fehlschluss des unverleihbaren Geldes

Da es zu einer zukünftigen Abwertung des Geldes kommt, muss die Fisher-Gleichung[1] benutzt werden, um eine kombinierte Wachstumsrate innerhalb des Geldes zu berechnen, welches selbst der Inflation[2] unterliegt. Dadurch wird der Nominalzins angepasst, um den Realzins zu erhalten. Die Darstellung wird vereinfacht, indem anstelle von Zinssätzen Verhältnisse verwendet werden. Wie im Abschreibungsprinzip[3] gezeigt, beträgt die Wachstumsrate von Warengeld 0 %, oder es hat eine Wachstumsquote von 100 %.

Monopolgeld[4] weist aufgrund seiner Seigniorage[5] eine Wertminderung auf.

```
Monopolgeld-Wachstumsverhältnis = Warengeld-Wachstumsverhältnis /
Seigniorage-Verhältnis
100% / 103% = ~97%
```

Geld mit fester Menge könnte aufgrund von Preisdeflation[6] an Wert gewinnen.

```
Fest-Angebot-Geld-Wachstumsverhältnis = Warengeld-Wachstumsverhältnis /
Inflationsverhältnis
100% / 97% = ~103%
```

Es wird angenommen, dass sich die Kaufkraft[7] eines Geldes mit festem Angebot proportional zu den Produkten ändert, die es repräsentiert (d. h. der Nachfrage). Mit

Referenzen

[1] https://de.wikipedia.org/wiki/Fisher-Gleichung

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] Kapitel: Abschreibungsprinzip

[4] Kapitel: Taxonomie des Geldes

[5] https://de.wikipedia.org/wiki/Seigniorage

[6] https://de.wikipedia.org/wiki/Deflation

[7] Kapitel: Inflationsprinzip

anderen Worten, bei der doppelten Produktmenge wird jede Einheit des Geldes für die doppelte Produktmenge gehandelt.

```
Kaufkraft-Dieses-Jahr = Kaufkraft-Letztes-Jahr * Jährliches-
Wachstumsverhältnis
100 * 103% = 103
```

Die Annahme einer Deflation des Preises für hartes Geld beruht auf der Annahme eines positiven Wirtschaftswachstums. Im Falle einer wirtschaftlichen Kontraktion weist das Geld eine Preisinflation[1] auf. Im Falle von Wirtschaftswachtum (zunehmender Wohlstand) bedeutet dies, dass die Zinsen die Abwertung übersteigen. Sowohl die Zinsen als auch die Abwertung müssen immer positiv sein, wie die Zeitpräferenz[2] impliziert.

```
Zinsverhältnis > Abwertungsverhältnis > 100%
Zinsverhältnis / Wachstumsverhältnis = Abwertungsverhältnis
Zinsverhältnis / Wachstumsverhältnis > 100%
Zinsverhältnis > Wachstumsverhältnis
```

Eine wirtschaftliche Kontraktion (abnehmender Wohlstand) führt zu steigenden Zinsen, wie die Grenznutzentheorie[3] es impliziert, bis wieder positives Wachstum herrscht. Somit ist eine solche Kontraktion ein selbstkorrigierender Zustand.

```
Abwertungsverhältnis > Zinsverhältnis > 100%
Zinsverhältnis / Wachstumsverhältnis = Abwertungsverhältnis
Zinsverhältnis / Wachstumsverhältnis > 100%
Zinsverhältnis > Wachstumsverhältnis
```

Beachten Sie, dass sowohl bei Wirtschaftswachstum als auch bei Konjunkturrückgang die Zinsen das Wachstum übersteigen müssen, da Kreditvergabe die einzige Wachstumsquelle ist. Da Wachstum die einzige Grundlage der Deflation in einer

Referenzen

[1] https://de.wikipedia.org/wiki/Inflation

[2] Kapitel: Zeitpräferenzfehlschluss

[3] https://de.wikipedia.org/wiki/Grenznutzen

deflationären Geldmenge ist, stellt das Horten des Geldes eine Geldentwertung (Verbrauch) dar.

Es gibt eine Theorie, dass es ökonomisch irrational ist, deflationäres Geld zu verleihen. **Wie gezeigt wurde, ist es rational, jedes Geld zu verleihen, auch deflationäres, was die Theorie widerlegt.** Jedes gegenteilige Verhalten impliziert einen rein spekulativen Zustand[1], der nicht durch die Tatsache eines festen Angebots gestützt wird.

Referenzen

[1] Kapitel: Spekulativer Konsum

PREIS

Mondfehlschluss

Es gibt eine Theorie, dass das Horten von Bitcoin einen andauernden Gewinn garantiert. Die Theorie basiert auf den folgenden ökonomischen Gesetzen.

- Ein Geld ist besser als zwei (Metcalfesches Gesetz[1])
- Besseres Geld verdrängt andere Währungen (Thiers Gesetz[2])
- Bei festem Angebot steigt der Preis mit der Nachfrage (Gesetz von Angebot und Nachfrage[3])
- Der potenzielle Anstieg der Nachfrage ist unbegrenzt (Handel ist in der Summe positiv)

Das Horten ist reine Spekulation, alle Erträge stellen Gewinn oder Verlust dar. Das Geld wird nicht gegen Zinsen an jemanden verliehen und steht daher jederzeit zum Umtausch zur Verfügung, ein Vorteil, der den entgangenen Zinssatz ausgleicht.

Eine Konsequenz aus dieser Theorie ist, dass keine Investitionen in die Produktion erforderlich sind, um davon zu profitieren. Für jede Produktion ist Kapital erforderlich. Kreditgeber (Investoren) erhalten Zinsen im Austausch für Zeit ohne ihr Kapital. **Produktion ist die Quelle des Handels und daher resultiert jede wirtschaftliche Aktivität aus Investitionen.** Ein Hort wird durch das Ausbleiben von Konsum in der Produktion definiert. Wenn alle Menschen ihr Kapital horten würden, gäbe es nichts zu handeln und daher keine Nachfrage nach dem Geld.

Referenzen

[1] https://de.wikipedia.org/wiki/Metcalfesches_Gesetz

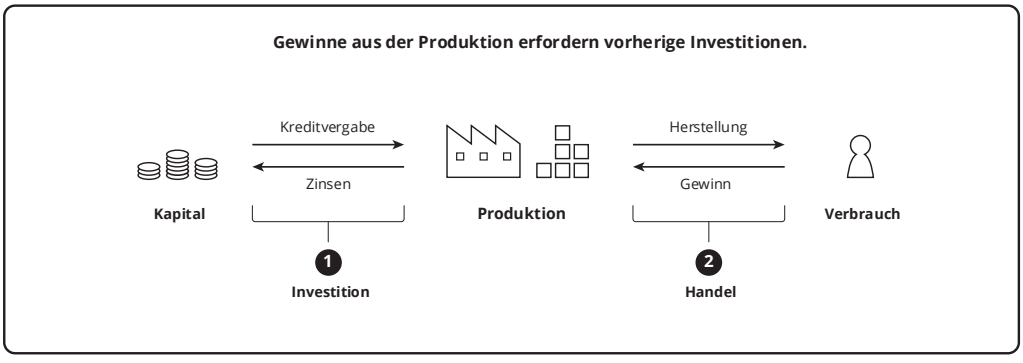
[2] https://de.wikipedia.org/wiki/Greshamsches_Gesetz#Umkehrung

[3] https://de.wikipedia.org/wiki/Marktgleichgewicht

Es scheint, dass die Theorie irrational ist und die Idee unterstützt, dass Bitcoin tatsächlich Magic Internet Money[1] ist. Wenn eine Theorie zu einem Widerspruch führt, ist die Theorie fehlerhaft. Ein Marktgeld mit festem Angebot[2] kann nur aufgrund folgender Faktoren an Kaufkraft gewinnen:

1. Wirtschaftswachstum – Schaffung von mehr Nachfrage zur Verwendung des Geldes im Handel
2. Monetarisierung – Menschen übertragen Nachfrage von anderem Geld

Doch Wirtschaftswachstum ist ausschließlich das Ergebnis von Investitionen. Wachstum ist zwangsläufig[3] geringer als die Kapitalrendite (Zinsen), und vollständiges Horten ist überhaupt keine Investition. Und natürlich hat die Monetarisierung eine Grenze. Schließlich berücksichtigt die Theorie die Stabilitätseigenschaft[4] von Bitcoin nicht. Aus diesen Gründen ist die Theorie ungültig.



Referenzen

[1] https://medium.com/@paulbars/magic-internet-money-how-a-reddit-ad-made-bitcoin-hit-1000-and-inspired-south-parks-art-b414ec7a5598

[2] Kapitel: Taxonomie des Geldes

[3] Kapitel: Abschreibungsprinzip

[4] Kapitel: Stabilitätseigenschaft

Preisschätzung

Die potenzielle Kapitalisierung und damit der potenzielle Stückpreis von Bitcoin wird auf verschiedene Weise geschätzt. Ein gängiger Ansatz besteht darin, sich vorzustellen, dass Bitcoin sämtliches staatliche Geld[1] oder sogar das Bruttoweltprodukt[2] ersetzt. Andere Ansätze, die Modelle vergangener Preise[3] verwenden, um zukünftige Preise vorherzusagen, sind wirtschaftlich irrational[4] und werden daher hier nicht berücksichtigt. Die Annahme, dass Bitcoin eine Reservewährung[5] sein könnte, wird aus Gründen verworfen, die im Fehlschluss der Reservewährung[6] erörtert werden. Die Auswirkungen spekulativer Hortung auf den Preis werden aufgrund der katallaktischen[7] Widerlegung der Spekulation als Preisdeterminante[8] nicht berücksichtigt.

Da Bitcoin Geld[9] und kein Kredit ist, ist der „Geld-Ansatz" die rationalere Ausgangsannahme. Ohne ein klares Verständnis des wesentlichen Unterschieds zwischen Geld und Kredit ist dieser Ansatz in der Praxis jedoch oft fehlerbehaftet. Wie im Fehlschluss der Kreditausweitung[10] gezeigt, kann Bitcoin die Kreditausweitung nicht begrenzen. Wenn er die Kreditausweitung (hypothetisch) eliminieren würde, gäbe es überhaupt keine Produktion und er wäre nichts wert. Die rationalste Ausgangsannahme in Bezug auf die Kreditausweitung ist, dass Bitcoin zum gleichen Zinssatz reserviert wird

Referenzen

[1] https://www.fool.com/investing/2017/05/25/could-the-price-of-bitcoin-go-to-1-million.aspx

[2] https://de.wikipedia.org/wiki/Bruttoinlandsprodukt#Bruttoweltprodukt_und_Wirtschaftskraft

[3] https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

[4] Kapitel: Bestand-zu-Zufluss-Fehlschluss

[5] Kapitel: Reserveprinzip

[6] Kapitel: Fehlschluss der Reservewährung

[7] https://de.wikipedia.org/wiki/Katallaktik

[8] https://mises.org/online-book/man-economy-and-state-power-and-market/2-direct-exchange/7-speculation-and-supply-and-demand-schedules

[9] Kapitel: Taxonomie des Geldes

[10] Kapitel: Fehlschluss der Kreditausweitung

wie andere Gelder. Die Rate der Kreditausweitung wird allein durch die menschliche Zeitpräferenz[1] bestimmt, daher ist es eine Annahme, dass die Produktion dadurch mit den historischen Normen übereinstimmt.

Betrachten wir fünf mögliche Optionen für den „Geld-Ersatz" durch Bitcoin:

- Materielles Geld.
- Basisgeld (M0).
- Bankkredit (M3-M0).
- Alle Kredite (Bank, Schulden, Eigenkapital).
- Bruttoweltprodukt.

Ausschließlich materielles Geld („Tresorgeld") zu verwenden, ist ein irrationaler Ansatz. Das Geld, das als Geldäquivalent verbucht wird, muss auch einbezogen werden, wenn man greifbares Geld betrachten will, da es sich bei beiden um dasselbe Angebot handelt. Zentralbanken[2] drucken und prägen bei Bedarf materielles Geld auf der Grundlage der zu, erfüllenden „Verpflichtungen", und alle Kredite in diesem Geld werden auf dieser Basis ausgeweitet. Dieses Konzept wird im Staatsbankenprinzip[3] erörtert. Auch die Verwendung von Krediten ist ein irrationaler Ansatz, da Bitcoin kein Kredit ist. Als ein Geld wird es verwendet, um Kreditverpflichtungen zu begleichen[4]. Dieses Konzept wird im Fehlschluss der Schuldenschleife[5] erörtert. Aus demselben Grund ist es natürlich irrational, jede beliebige Kombination aus Geld und Kredit zu verwenden (wie etwa M1, M2 oder M3[6], da diese M0 einschließen). Auch das Bruttoprodukt ist für eine Substitution nicht vertretbar, da es weder Geld noch Kredit ist.

Referenzen

[1] Kapitel: Zeitpräferenzfehlschluss
[2] https://de.wikipedia.org/wiki/Zentralbank
[3] Kapitel: Staatsbankenprinzip
[4] https://de.wikipedia.org/wiki/Settlement_(Finanzwesen)
[5] Kapitel: Fehlschluss der Schuldenschleife
[6] https://en.wikipedia.org/wiki/Money_supply#United_States

Zum Vergleich wollen wir jedoch jede der fünf oben aufgeführten Optionen schätzen. Die Basiswerte für die folgende Tabelle sind US-Dollar-Beträge, die aus dem Fehlschluss der Kreditausweitung[1] entliehen wurden. Diese werden durch eine Schätzung der relativen Größe[2] der Weltwirtschaft nach Aktienmarktkapitalisierung erweitert. Der US-Markt macht ungefähr 40 % der globalen Märkte aus. Daher übersteigen diese Werte die US-Zahlen um einen Faktor von 1/40 %. Dies bevorzugt Einfachheit gegenüber Präzision, da das einzige Ziel darin besteht, eine rationale Schätzmethode zu demonstrieren. Die angenommene Menge an Bitcoin beträgt 18.952.500, da 95 % geschürft wurden (~10 Jahre in der Zukunft) und 5 % verloren gingen (z. B. hat Satoshi private Schlüssel verloren).

Die Bewertungen basieren auf Zahlen aus dem Jahr 2019, die Bitcoin-Inflation jedoch auf dem Jahr 2029. Dies bedeutet, dass die Werte aufgrund der Annahme von Wirtschaftswachstum und US-Dollar-Geldinflation[3] höher sein sollten. Letztere kann eliminiert werden, indem man dies als konstante Dollar-Projektion für 2019 betrachtet. Unter der Annahme eines realen Wirtschaftswachstums[4] von 2 % über 10 Jahre wurden die Werte für 2029 um ~22 % erhöht.

Referenzen

[1] Kapitel: Fehlschluss der Kreditausweitung

[2] https://seekingalpha.com/article/4202768-u-s-percent-world-stock-market-cap-tops-40-percent

[3] https://en.wikipedia.org/wiki/Monetary_inflation

[4] https://de.wikipedia.org/wiki/Wirtschaftswachstum

Ersatz	Umfang (2019)	USD/BTC (2029)
Materielles Geld	4.347.460.000.000 $	279.852 $
Basisgeld	8.187.102.500.000 $	527.016 $
Bankkredit	36.018.735.000.000 $	2.318.578 $
Gesamtkredit	236.812.492.891.206 $	15.243.965 $
Bruttoweltprodukt	80.270.000.000.000 $	5.167.097 $

Die Schätzung für den Ersatz des globalen Basisgeldes beträgt 527.016 US-Dollar. Die Ermittlung des Nettobarwertes[1] erfordert eine Schätzung der Kapitalkosten. Die Verwendung eines konservativen Wertes von 7,2 % Zinsen impliziert[2] 100 % Opportunitätskosten[3] für die Spekulation über einen Zeitraum von ca. 10 Jahren oder einen gegenwärtigen Preis von 263,508 US-Dollar.

Nun betrachten wir die primäre Annahme, nämlich den Ersatz allen Geldes. Bitcoin bietet keinen Schutz[4] gegen staatliche Verbote seiner Verwendung im Handel. Unter der Annahme, dass die Staaten Seigniorage[5] und Zensur beibehalten wollen, könnten wir mit dem Anteil des globalen Schwarzmarktes multiplizieren, der auf etwa 28 % des globalen Marktes geschätzt[6] wird. Die Basisgeldschätzung umfasst *alle* Marktaktivitäten in dem Geld (Kreditschätzungen tun dies nicht). Bei einem 100-prozentigen Ersatz des geschätzten Schwarzmarkthandels beträgt der Preis 73.782 US-Dollar.

Referenzen

[1] https://de.wikipedia.org/wiki/Kapitalwert

[2] https://de.wikipedia.org/wiki/72er-Regel

[3] https://de.wikipedia.org/wiki/Opportunitätskosten

[4] Kapitel: Prinzip der Genehmigungsfreiheit

[5] https://de.wikipedia.org/wiki/Seigniorage

[6] https://voxeu.org/index.php?q=node/7964

Unter der Annahme, dass staatliche Gelder ausschließlich auf dem weißen Markt verwendet werden, können wir nicht davon ausgehen, dass 100 % der Schwarzmarktaktivitäten auf Bitcoin entfallen. Es gibt keine offensichtliche Grundlage für die Schätzung dieses Anteils, aber **der Preis von ~10.000 US-Dollar im Jahr 2019 impliziert eine prognostizierte Schwarzmarktakzeptanz von ~7,4 % im Jahr 2029.**

Diese Schätzung berücksichtigt Bitcoins Stabilitätseigenschaft[1] nicht. Es ist möglich, dass der Handel zu monetären Ersatzmitteln[2] gezwungen wird, bevor die derzeit angenommene zukünftige Adoption erreicht werden kann.

Referenzen

[1] Kapitel: Stabilitätseigenschaft

[2] Kapitel: Substitutionsprinzip

Knappheitsfehlschluss

Als *absolutes* Konzept bedeutet wirtschaftliche Knappheit[1] einer Ressource lediglich, dass sie nicht unbegrenzt verfügbar ist. Hinzu kommt, dass auch eine knappe Ressource keinen Wert hat, wenn niemand sie nachfragt. Eine knappe Ressource, für die Nachfrage besteht, ist Eigentum. Es wird kein Schwierigkeitsgrad bei der Produktion der Ressource vorausgesetzt.

Knappheit kann sich auch auf die *relative* Verfügbarkeit einer Eigenschaft beziehen. Bei einem gegebenen Angebot bedeutet eine steigende Nachfrage eine sinkende Verfügbarkeit (zunehmende Knappheit). Eine steigende Nachfrage führt jedoch tendenziell zu einer steigenden Produktion und damit zu einer steigenden Verfügbarkeit. Ebenso impliziert bei gegebener Nachfrage ein steigendes Angebot eine steigende Verfügbarkeit (abnehmende Knappheit). Ein steigendes Angebot führt jedoch tendenziell zu einer geringeren Produktion und damit auch zu geringerer Verfügbarkeit. Diese negativen Rückkopplungen stabilisieren die Verfügbarkeit und dementsprechend den Preis.

Ein einzelner Coin hat ein festes Angebot[2]. Es gibt eine Theorie, dass das feste Angebot von Bitcoin die Quelle seines Wertes sei. Wie bei Bitcoin gibt es auch ein festes Angebot von Mona Lisas[3], nur eine ist möglich. Die Theorie besagt, dass dies die Quelle des Wertes des berühmten Kunstwerks ist. Es gibt jedoch zahllose einzigartige Kunstwerke, für die es keine Nachfrage gibt und die daher keinen Wert haben. **Der Wert von Bitcoin kann nicht aufgrund absoluter Knappheit steigen.** Im Gegenteil, je höher der Wert, desto knapper wird er. Verbreitung ist keine wichtige monetäre Eigenschaft, außer in Bezug auf Portabilität und Teilbarkeit.

Referenzen

[1] https://de.wikipedia.org/wiki/Knappheit

[2] Kapitel: Inflationsprinzip

[3] https://en.m.wikipedia.org/wiki/Mona_Lisa

Ein Aspekt der Theorie ist, dass das feste Angebot von Bitcoin die Quelle seines Nutzens ist, da es eine nicht zunehmende Verfügbarkeit gewährleistet. Dies erfordert jedoch eine nicht abnehmende Nachfrage. Bitcoin ist im Bereich des Eigentums einzigartig, da die Kosten für den Transfer von Natur aus mit der Nachfrage nach Transfers steigen. Dies erzeugt effektiv dieselbe negative Nachfragerückkopplung[1], die bei Eigentum ohne festes Angebot auftritt.

Im Gegensatz zur Mona Lisa unterliegt sie auch der wirksamen Substitution[2]. Da eine nicht abnehmende Nachfrage nicht garantiert ist, ist die Theorie ungültig. Wie bei wirtschaftlichen Fehlschlüssen üblich, liegt der Fehler teilweise darin begründet, dass nur eine Seite der Angebots-Nachfrage-Beziehung betrachtet wird.

Eine weitere Fehlerursache ist eine Fehlinterpretation des Verhaltens von Warengeldern. Aufgrund seiner geringeren Verbreitung auf der Erdoberfläche ist Gold in alltäglichen Szenarien portabler[3] geblieben als häufiger vorkommende Materialien wie Eisen und Salz. Die Portabilität von elektronischem Geld[4] ist jedoch unabhängig von der Anzahl der existierenden Einheiten. Abgesehen von einer ausreichenden Teilbarkeit ist die Gesamtzahl der Bitcoin-Einheiten völlig willkürlich und hat daher keinen Bezug zu ihrem Nutzen.

Eine weitere Fehlerursache ist eine Fehlinterpretation des Verhaltens staatlicher Gelder. Durch Gesetze gegen Geldfälschung[5] kontrolliert der Staat die Geldmenge, indem er den Wettbewerb einschränkt. Er kann daher eine Inflationssteuer[6] erheben, indem er die Menge erhöht, ohne viel Kapital in der Produktion zu verbrauchen, und so das Verhältnis

Referenzen

[1] Kapitel: Stabilitätseigenschaft

[2] Kapitel: Substitutionsprinzip

[3] https://en.wikipedia.org/wiki/Money#Properties

[4] Kapitel: Taxonomie des Geldes

[5] https://de.wikipedia.org/wiki/Falschgeld

[6] https://de.wikipedia.org/wiki/Seigniorage

von Geld zu Kapital erhöht. Ohne eingeschränkten Wettbewerb würde die Menge durch Marktkräfte als Reaktion auf die Nachfrage steigen, was die Steuern eliminieren würde. Mit anderen Worten, das Geld würde sich wie eine weit verbreitete Ware verhalten, die allerdings schlecht übertragbar wäre (zumindest bis dies vom Staat vergütet würde). Schlechte Transportierbarkeit ist oft eine tatsächliche Folge der Hyperinflation.

Knappheit ist eine Funktion von Angebot und Nachfrage und kann daher Geld nicht inhärent sein, selbst bei festem Angebot. Sowohl Warengeld als auch Bitcoin eliminieren die Inflationssteuer, obwohl Warengeld der negativen Rückkopplung der Geldinflation und Bitcoin der negativen Rückkopplung des Gebührendrucks unterliegt.

Stabilitätseigenschaft

Wert ist subjektiv[1] und daher ist Preisstabilität eine ökonomische Fiktion. Die Wechsel-Kurse eines Geldes werden durch Angebot und Nachfrage[2] bestimmt, die wiederum von den Nachfrageplänen aller Menschen für alle Produkte bestimmt wird. Die Stabilität eines Geldes ist nicht eine Tendenz zu konstanten Preisen in allen anderen Dingen, sondern ein dämpfendes[3] Verhältnis zwischen der Nachfrage nach dem Geld und seinem Angebot.

Wir können Gelder in drei verschiedene Versorgungskategorien einteilen:

- Marktangebot (Commodities[4] und früher Bitcoin)
- Monopolangebot (Monopol[5])
- Festgelegtes Angebot (später Bitcoin[6])

In jedem Geld verringert die Zerstörung von Einheiten das Angebot und erhöht daher den Wert der verbleibenden Einheiten. Da es keinen finanziellen Anreiz für Verluste gibt, wirkt sich dies nicht auf die Stabilität aus.

Die Marktgeldmenge erhöht sich aufgrund des finanziellen Anreizes, mehr zu produzieren[7], wenn der Preis bei oder über den Produktionskosten (einschließlich Kapitalkosten) erwartet wird. Wie in Inflationsprinzip[8] gezeigt, ist das Verhältnis

Referenzen

[1] https://en.wikipedia.org/wiki/Subjective_theory_of_value
[2] https://de.wikipedia.org/wiki/Marktgleichgewicht
[3] https://de.wikipedia.org/wiki/Dämpfung
[4] https://de.wikipedia.org/wiki/Commodities
[5] Kapitel: Taxonomie des Geldes
[6] https://de.wikipedia.org/wiki/Bitcoin
[7] https://de.wikipedia.org/wiki/Gold#Gewinnung
[8] Kapitel: Inflationsprinzip

zwischen Angebot und Nachfrage (Preis) stabil, obwohl das Angebot nicht festgelegt ist. Der Wettbewerb stellt sicher, dass die Marktgeldproduktion durch die Nachfrage gesteuert wird. Die Rückkopplung eines Nachfragerückgangs infolge einer Angebotssteigerung verringert den Produktionsanreiz und sorgt so für Stabilität.

Als Marktgeld hat die Erhöhung des Bitcoin-Angebots keinen Einfluss auf den Preis. Da die Angebotsrate jedoch fest ist, basiert seine Stabilität stattdessen auf Änderungen der Nachfrage. Im Gegensatz zu Warengeld steigen und fallen die Kosten für die Herstellung von Bitcoin je nach Nachfrage. Da der Preis das Verhältnis zwischen Angebot und Nachfrage darstellt, hat dies den gleichen Effekt. Der Zweck der Geldinflation von Bitcoin besteht darin, Einheiten rational zu verteilen, und wird so schließlich ausgephast.

Die Menge des Monopolgeldes wird durch den Souverän[1] aufgrund der finanziellen Belohnung der Seigniorage[2] willkürlich erhöht (oder zur Umlaufsicherung[3] besteuert).

Wenn die Monopolgeldinflation vorhersehbar ist, kann sie kapitalisiert werden, wodurch die Rendite der Seigniorage diskontiert wird. Daher werden Angebotsänderungen häufig nicht veröffentlicht[4]. Aufgrund des Schutzes durch das Staatsmonopol[5] (d.h. die Herstellung ist ein Fälschungsdelikt), kann der Wettbewerb die Renditen nicht wirksam begrenzen. Der daraus resultierende hoheitliche Gewinn (Steuern) ist der Lohn der Seigniorage und die Rechtfertigung für Monopolgeld[6]. Der Monopolschutz ist die einzige ökonomische Unterscheidung zwischen Waren- und Monopolgeld. Der durch Seigniorage verursachte Angebotsanstieg wird nur durch

Referenzen

[1] https://de.wikipedia.org/wiki/Souverän

[2] https://en.wikipedia.org/wiki/Seigniorage

[3] https://de.wikipedia.org/wiki/Umlaufgesichertes_Geld

[4] https://www.reuters.com/article/us-venezuela-economy/crisis-hit-venezuela-halts-publication-of-another-major-indicator-idUSKBN16S1YF

[5] https://de.wikipedia.org/wiki/Staatsmonopol

[6] Kapitel: Reserveprinzip

politische Unruhen gemildert, da sich die Menschen gegen den daraus resultierenden Wertverlust wehren. Diese Unruhe manifestiert sich zunächst als Kapitalflucht[1], der mit Devisenverkehrsbeschränkung[2] begegnet wird.

Als Geld mit festgelegtem Angebot bleibt der späte Bitcoin stabil. Da die Gebühren zwangsläufig mit der Nachfrage steigen, eliminiert der Nutzenschwellenwert[3] die Nachfrage nach Transaktionen mit einem Wert unterhalb des Schwellenwertes. Allgemeiner gesprochen, das Gebührenniveau steigt bis zu dem Punkt, an dem monetäre Ersatzstoffe[4] für eine Transaktion mit einem bestimmten Wert kostengünstiger sind. **Stabilität ergibt sich daher aus der direkten Begrenzung der Nachfrage, im Gegensatz dazu, dass man sich dabei auf eine Erhöhung des Angebots verlässt.** Stabilität impliziert, dass der Preis begrenzt ist, er aber dennoch mit zunehmender effektiver Transaktions-Tragfähigkeit[5] des Coins und mit erhöhtem Nutzen relativ zu Substituten steigen kann.

Referenzen

[1] https://de.wikipedia.org/wiki/Kapitalflucht

[2] https://de.wikipedia.org/wiki/Devisenverkehrsbeschränkung

[3] Kapitel: Eigenschaft der Nutzenschwelle

[4] Kapitel: Substitutionsprinzip

[5] Kapitel: Skalierungsprinzip

Bestand-zu-Zufluss-Fehlschluss

Bestand-zu-Zufluss[1] (Stock-to-Flow) beschreibt historisch die Beziehung zwischen Kapital und Einkommen und ermöglicht die Schätzung eines zukünftigen Kapitalniveaus anhand eines erwarteten Einkommensniveaus. Später wurde dieses elementare Konzept allgemein auf die Geldmenge angewendet.

Das Verhältnis von Bestand zu Zufluss ist ein Zeitmaß. Bei einem höheren Verhältnis steigt der Bestand langsamer an. Es gibt eine Theorie, dass Geld mit einem höheren inhärenten Bestand-zu-Zufluss-Verhältnis weniger proportionale Geldinflation[2] erleidet als Geld mit einem niedrigeren Verhältnis. Die Theorie besagt, dass ein höheres Verhältnis ein „härteres" Geld bedeutet, das als von Natur aus widerstandsfähiger gegen die Auswirkungen der Geldinflation definiert ist.

Die Theorie berücksichtigt den Ursprung der Zufluss-Raten nicht. Sie geht zwangsläufig davon aus, dass die Produktionsrate einfach eine Eigenschaft der Substanz ist. Aber die Produktion von allem findet dann statt, wenn der erwartete Preis die Produktion rentabel macht. Ein höheres Gewinnpotential führt zu mehr Wettbewerb und beschleunigt die Angebotssteigerung. Mehr Menschen, die nach Gold graben, erhöhen dessen Zufluss.

Mit anderen Worten, der Fluss ist eine Funktion der Nachfrage. Ein erwarteter Verlust führt zu keinerlei Produktion. Dieser Mangel an Fluss ist *nicht inhärent in der Substanz*, sondern eine *Folge mangelnder Nachfrage*. Da sowohl Angebot als auch Nachfrage den Fluss bestimmen, ist die Theorie ungültig. Dieser seit langem bekannte[3] Fehler ist kein

Referenzen

[1] https://en.wikipedia.org/wiki/Stock_and_flow

[2] https://en.wikipedia.org/wiki/Monetary_inflation

[3] https://mises.org/online-book/theory-money-and-credit/ii-fluctuations-objective-exchange-value-money-evoked-changes-ratio-between-supply-money-and-demand-it/6-quantity-theory

Aspekt des elementaren Bestand-zu-Zufluss-Konzepts, sondern eine falsche Anwendung desselben.

Aufgrund der Fälschungsgesetze ist der Wettbewerb um die Produktion staatlichen Geldes eingeschränkt, was dem Staat eine von Marktkräften unabhängige Kontrolle des Angebots ermöglicht. Wie bei anderen Geldern sind Angebot und Nachfrage im Allgemeinen unvorhersehbar. Ein Staat kann die Emission seiner Reservenoten[1] an ein anderes Geld, wie z.B. Gold „koppeln". Diese Beziehung kann sogar über viele Jahrzehnte bestehen bleiben. In diesem Fall würde das Bestand-zu-Zufluss-Verhältnis fälschlicherweise eine mit Gold vergleichbare „Härte" anzeigen.

Da es sich beim Bestand-zu-Zufluss-Verhältnis von Geld um die umgekehrte monetäre Inflationsrate handelt, ist dessen Beziehung zur Geldinflation tautologisch. Es sagt nichts über die zukünftige Geldinflation aus. Es kann verwendet werden, um historische Beziehungen zu analysieren und zukünftige Bestände auf der Grundlage *angenommener* zukünftiger Ströme zu berechnen, aber es kann nicht verwendet werden, um die zukünftige Geldinflation *vorherzusagen*. Jede Aussage, dass eine Spekulation auf der Grundlage historischer Bestand-zu-Zufluss-Verhältnisse profitabler sein wird als eine andere, ist ein Fehler.

Referenzen

[1] Kapitel: Reserveprinzip

SKALIERUNG

Überprüfbarkeitsfehlschluss

Die Zahlungsfähigkeit eines Bitcoin-Verwahrers (Treuhänder) kann nicht geprüft werden. Ein Verwahrer ist eine Person mit Ermessensspielraum sowohl bei der Freigabe eines Vermögenswerts als auch bei der Ausgabe von Wertpapieren gegen denselben. Wenn sowohl die Freigabe des Vermögenswerts als auch die Ausgabe von Wertpapieren gegen ihn durch Konsensregeln kontrolliert werden, handelt es sich in Wirklichkeit nicht um eine Verwahrungsbeziehung. Dies ist der Unterschied zwischen einer Reserve[1] und einer Zusatzebene. Eine Ebene wird durch ein Protokoll erzwungen (nicht-verwahrend) und muss daher nichts prüfen.

Eine Solvenzprüfung erfordert einen gleichzeitigen (atomaren) Nachweis sowohl des vollen Betrags des von einem Verwahrer gehaltenen Vermögenswerts als auch der dagegen ausgegebenen Wertpapiere. Im Falle einer nationalen Bitcoin-Reserve würde dies einen vollständigen Nachweis aller gegen die Reserve ausgegebenen Fiatgelder (z. B. der Sicherheit) sowie der in der Reserve gehaltenen Bitcoin erfordern. Selbst wenn das Wertpapier in einer separaten öffentlichen Blockchain wird, ist die Atomizitätsanforderung nicht erfüllt.

In manchen Fällen kann es als ausreichend angesehen werden, die Atomizitätsanforderung außer Acht zu lassen und Fehler in Kauf zu nehmen, in der Annahme, dass wesentliche Abweichungen irgendwann entdeckt würden. Im Falle des Staatsbankwesens[2] reicht es jedoch nicht aus, die Abweichungen aufzudecken. Historisch gesehen war es nicht schwierig, solche Abweichungen aufzudecken. Die Schwierigkeit besteht darin, sie zu stoppen.

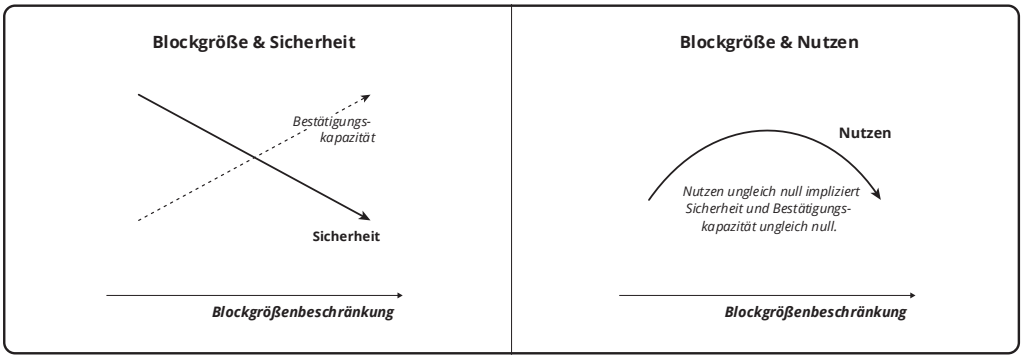
Referenzen

[1] Kapitel: Reserveprinzip

[2] Kapitel: Fehlschluss der Reservewährung

Skalierungsprinzip

Skalierbarkeit[1] ist die proportionale Erhöhung einiger Leistungsaspekte, wenn mehr Hardware eingesetzt wird. Der Transaktionsdurchsatz von Bitcoin ist absolut nicht skalierbar, da er durch keine Menge an zusätzlicher Hardware erhöht werden kann.

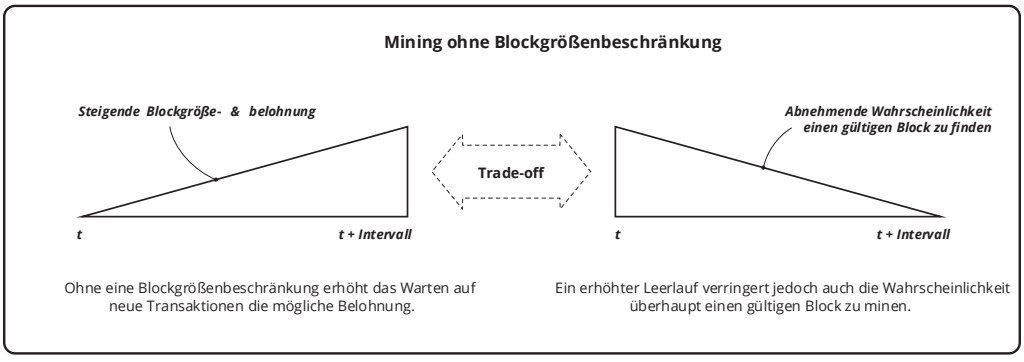


Die Konsensregel zur Blockgrößenbegrenzung legt den willkürlichen Kompromiss zwischen Nutzen und Systemsicherheit fest. Eine erhöhte Blockgröße erhöht den Transaktionsdurchsatz und daher die Ressourcenkosten der Transaktionsvalidierung (d.h. Verarbeitung, Speicherung und Bandbreite). Da die Validierungskosten steigen, wird die wirtschaftliche Sicherheit durch ein erhöhtes Zentralisierungsrisiko[2] beeinträchtigt. Da der Kompromiss willkürlich ist, gibt es keine ideale Größe.

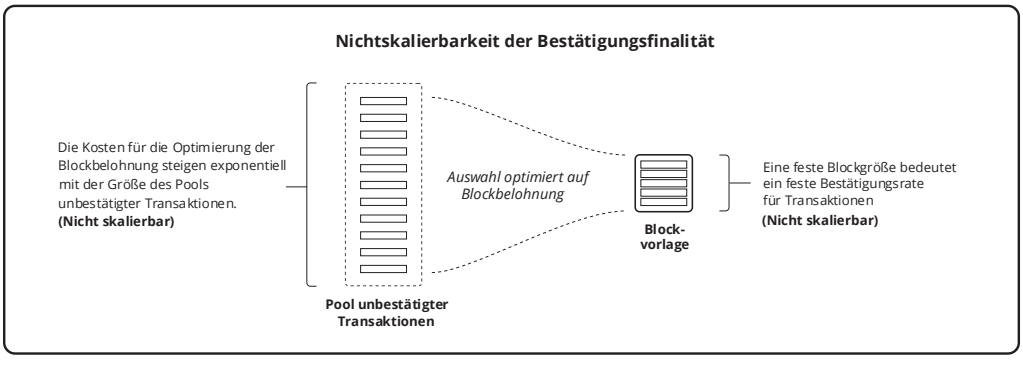
Referenzen

[1] https://de.wikipedia.org/wiki/Skalierbarkeit

[2] Kapitel: Zentralisierungsrisiko



Bei jeder Blockgröße bleibt das System aufgrund der Notwendigkeit der Bestätigungsendgültigkeit nicht skalierbar. Es muss eine endliche Menge von Transaktionen ausgewählt werden, was impliziert, dass andere möglicherweise ausgeschlossen werden. Dieser Ausschluss ist finanziell durch die Opportunitätskosten[1] motiviert, die entstehen, wenn das eingesetzte Miningkapital nicht genutzt wird, und ist Ausdruck der Nichtskalierbarkeit. Diese inhärente Grenze erfordert einen wettbewerbsorientierten Markt für Bestätigung und finanziert diesen im Verhältnis zur Nachfrage nach dem Geld[2].

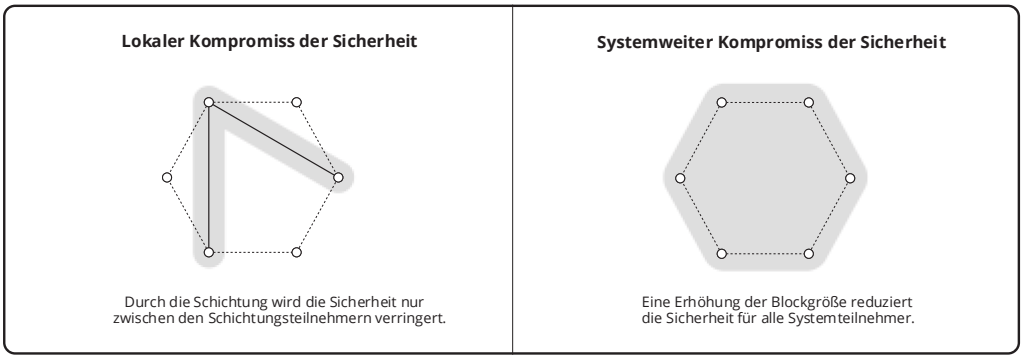


Referenzen

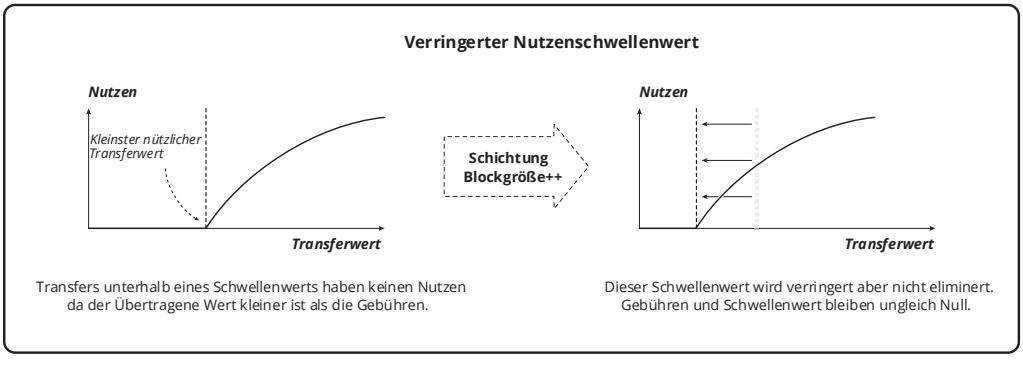
[1] https://de.wikipedia.org/wiki/Opportunitätskosten

[2] Kapitel: Taxonomie des Geldes

Die effektive Transaktions-Tragefähigkeit und daher der Nutzen können durch Zusatzebenen (Layering) erhöht werden. Dies stellt eine *lokal* und *zeitlich begrenzte* Beeinträchtigung der Sicherheit dar, im Gegensatz zur *systemweiten* und *dauerhaften* Sicherheitsbeeinträchtigung durch zunehmende Blockgröße.



Beide Kompromisse senken den Nutzenschwellenwert[1], beseitigen ihn jedoch nicht, was bedeutet, dass die Stabilitätseigenschaft[2] erhalten bleibt.



Referenzen

[1] Kapitel: Eigenschaft der Nutzenschwelle

[2] Kapitel: Stabilitätseigenschaft

Daher bestehen Stabilität und Nichtskalierbarkeit bei jeder Blockgröße und Anzahl von Zusatzebenen.

Substitutionsprinzip

Ein Substitutionsgut[1] ist ein Produkt, das anstelle eines anderen verwendet werden kann. Wenn der Preis eines Produktes steigt, wechseln die Menschen irgendwann zu Ersatzprodukten oder stellen die Nutzung gänzlich ein.

Während ein Ersatzprodukt zum gleichen Preis wie das Originalprodukt weniger wünschenswert wäre, gleicht sein niedrigerer Preis diese Präferenz aus. Auf diese Weise verringert die Verfügbarkeit von Ersatzprodukten die Nachfrage nach dem Originalprodukt. Das Ersatzprodukt konkurriert mit dem Originalprodukt, ebenso wie ein erhöhtes Angebot des Originalprodukts.

Wenn ein Coin ein festes Angebot hat, wird allgemein angenommen, dass keine Angebotssteigerung den Preisdruck nach oben verringern kann. Wie in der Stabilitätseigenschaft[2] gezeigt, integriert Bitcoin Transfergebühren, die zwangsläufig mit der Nutzung steigen. Diese einzigartige Eigenschaft erzeugt einen Preisdruck nach unten, indem sie die Nachfrage reduziert. **Aber diese steigenden Kosten machen auch Ersatzprodukte praktikabel und erzeugen einen Preisdruck nach unten, indem sie das Angebot effektiv erhöhen.**

Es gibt nichts, was die Entstehung mehrerer ähnlicher Coins verhindert. Es ist möglich, dass diese Währungen nahezu ununterscheidbare monetäre Eigenschaften aufweisen, wodurch der Trade-Off für den Austausch minimiert wird. Wie im Konsolidierungsprinzip[3] gezeigt, besteht immer ein Druck hin zu einer einheitlichen Währung, da dadurch die Wechselgebühren entfallen. Dieser Druck steht jedoch im

Referenzen

[1] https://de.wikipedia.org/wiki/Substitutionsgut

[2] Kapitel: Stabilitätseigenschaft

[3] Kapitel: Konsolidierungsprinzip

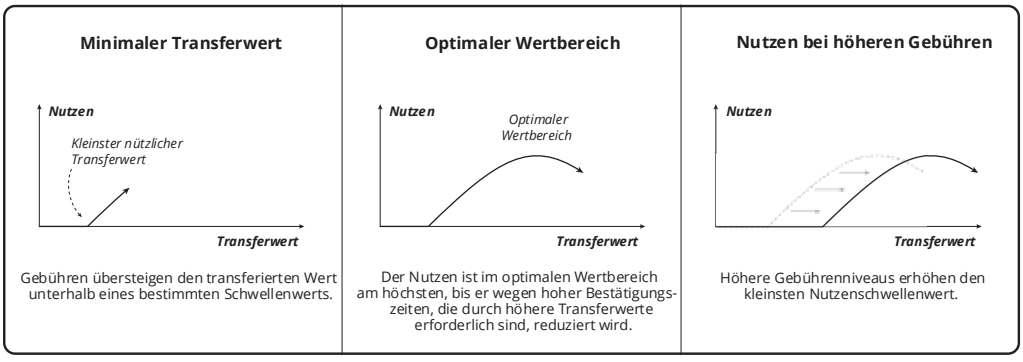
Widerspruch zu steigenden Kosten und muss ab einem bestimmten Grad der Nutzung der Substitution (oder Nichtnutzung) weichen.

Es gibt eine Theorie, dass, da die Schaffung neuer Coins nichts kostet, das Substitutionsprinzip impliziert, dass Bitcoin aufgrund der unbegrenzten kostenlosen Versorgung wertlos werden muss. Dabei wird die Tatsache außer Acht gelassen, dass die Leute für die Verwendung von Bitcoin zahlen müssen. Dies gilt für einen zweiten Coin genauso wie für den ersten.

Und ein steigendes Angebot mindert die Nachfrage. Irgendwann reicht die Nachfrage nicht mehr aus, um mehr Angebot zu produzieren/sicherzustellen, und daher ist die Theorie ungültig. Dies ist die gleiche Beziehung, die bei Warengeldern und tatsächlich bei allen Produkten gilt.

Eigenschaft der Nutzenschwelle

Der Nutzen drückt sich als Präferenz für einen Coin gegenüber Ersatzmitteln für Transfers eines vergleichbaren Wertes aus. Ein steigender Nutzen bedeutet ein steigendes Gebührenniveau, da von einem steigenden Transaktionsvolumen ausgegangen wird. Der Wettbewerb um Bestätigungen treibt die Gebühren in die Höhe. Angesichts der Unterschiede im Marktpreis der Gebühren über die Zeit kann man eine nicht wettbewerbsfähige Gebühr in Erwartung einer längeren Dauer zur Bestätigung anbieten. Andere werden keine Transaktionen auf der Blockchain durchführen und sich stattdessen auf Ersatzmittel verlassen.



Ein steigender Nutzen bedeutet daher einen steigenden durchschnittlichen Transferwert, da steigende Gebühren sonst dazu führen würden, dass die Transferkosten den transferierten Wert übersteigen. Eine größere Tiefe bedeutet eine höhere Bestätigungssicherheit. Daher kann Zeit gegen *höhere* Sicherheit vor Doppelausgaben eingetauscht werden. Die Zeit kann jedoch nicht unter eine Blockperiode reduziert werden, um eine *geringere* Sicherheit zu erreichen. Die niedrigsten Sicherheitsstufen sind keine (unbestätigt) und minimal (eine Bestätigung). Zwischen diesen Stufen kann kein Austausch stattfinden.

Höhere Gebühren bedeuten höhere Hash-Rate-Kosten, was den Bedarf nach Erhöhung der Bestätigungstiefe für den Transfer größerer Werte verringert. **Da es jedoch keine**

Möglichkeit gibt, die Sicherheit für Überweisungen mit geringerem Wert zu verringern, steigt der nützliche Mindestwert der Überweisung mit dem Nutzen. Wenn Überweisungen in einem bestimmten Wertebereich nicht unterstützt werden, bedeutet dies, dass Ersatzwährungen in diesem Bereich günstiger sind. Dies impliziert die Möglichkeit koexistierender Währungen zur Bedienung unterschiedlicher Wertebereiche. Allerdings weisen alle Bitcoins[1] diese Eigenschaft von Natur aus auf.

Regelunterschiede hinsichtlich der Blockperiode oder -Größe ändern an dieser Beziehung nichts. Die Auswirkungen dieser Münzvariationen sind streng proportional. Selbst Blöcke mit unbegrenzter Größe müssen Gebührenniveaus erzeugen, die Überweisungen mit geringem Wert ausschließen.

Referenzen

[1] Kapitel: Bitcoin-Etiketten

ANHANG

Glossar

Abrechnung

Die Bestätigung von geschichteten Transaktionen.

Aggregation

Die Tendenz zu geringerer Partizipation im Mining oder in der Validierung. Impliziert Kartellierung oder Zentralisierung.

Aktivierung

Start der Durchsetzung einer neuen Regel.

Angebot

Die Menge aller ausgegebenen Einheiten.

Angriff

Nutzung von Hash-Power zur Durchführung einer Doppelausgabe.

Anpassung

Eine Änderung der Schwierigkeit.

Anspruchsteller

Eine Person, welche Anspruch auf Eigentum hat, das unter der Kontrolle eines Treuhänders steht. Auch Pfandrechtinhaber, Anteilseigner, Kreditvergeber oder Einleger.

Arbeit

Der Prozess der Produktion eines Blocks.

Ausgang

Ein expliziter Transfer und ein Vertrag.

Ausgabe

Die initiale Veröffentlichung einer Transaktion.

Bekanntmachung

Die erste Kommunikation eines Blocks an eine andere Person.

Belohnung

Die Summe aus Subvention und Gebühren für einen Block.

Besitzer

Eine Person in der Kontrolle bestimmter Einheiten. Halter ist eine übliche Bezeichnung dafür.

Bestätigung

Aufnahme einer Transaktion in einen Block.

Befürwortung

Ein Skript, das einen Vertrag erfüllt. Signature-Script ist ein Anachronismus dafür.

Bitcoin

Die Menge an Grundsätzen, die einen Coin gegen den Staat absichern. Der Begriff und die Grundsätze werden durch Satoshi in “Bitcoin: Ein elektronisches Peer-To-Peer-Zahlungssystem” definiert.

Block

Eine gültige Menge an Transaktionen mit Zeitstempel und Nachweis.

Block-Pool

Die Menge schwacher Blöcke. Verwaister (Orphan-) Pool ist eine falsche Bezeichnung dafür.

Blockchain

Der Zweig mit dem größten kumulativen Beweis.

Blockhöhe

Die Anzahl der vorhergehenden Blöcke in einem Zweig.

Client-Server

Ein asymmetrisches Protokoll.

Coin

Ein Konsens über ein gegenseitig akzeptiertes Tauschmittel. BTC ist ein Coin.

Coinbase

Eine Transaktion, die eine Belohnung transferiert.

Deckelung

Die Begrenzung des Angebots über alle Zeit.

Delegation

Die Tendenz hin zu wenigen Eigentümern. Eigentümer haben direkte Kontrolle über die Ausgabe.

Denial of Service

Der Gebrauch von Kommunikation, um Schwachstellen im Protokoll oder der Implementierung auszunutzen, die die Leistung beeinträchtigen. DoS ist ein Akronym dafür.

Dezentralisierung

Die Tendenz gegen Zentralisierung.

Doppelausgabe

Die Befürwortung (Endorsement)desselben Ausgangsvertrags durch unterschiedliche Ausgaben.

Durchsetzung

Der Akt des Verwerfens ungültiger Daten.

Egoistisch

Ein Miner, der nicht ehrlich ist.

Ehrlich

Ein Miner, der auf dem Block eines anderen aufbaut.

Eingang

Ein Ausgangspunkt und eine Befürwortung.

Einheit

Die kleinste transferierbare Menge an Eigentum dargestellt durch einen Coin. Der Satoshi ist die Einheit von Bitcoin.

Entkoppeln

Eine Mine, die die Belohnung mit anderen teilt, um die Varianz zu reduzieren.

Entwickler

Eine Person, die eine Implementierung durchführt.

Kreditaufnahme

Der Handel zwischen Zeit mit Einheiten gegen den Besitz mit größerem Nutzen für den Kreditgeber.

Kandidat

Ein potenzieller Block mit unbestimmtem Nachweis.

Kapitalisierung

Das Produkt aus Preis und Angebot.

Kommunikation

Übertragung von Daten zwischen Maschinen.

Konsens

Eine Vereinbarung zwischen Personen. Außerdem die Menge an Personen, die an einer Vereinbarung beteiligt ist.

Konsensregeln

Menge der Nebenbedingungen, die einen Coin definieren.

Kooptierung

Verwendung von Aggression, um die Hash-Power zu kontrollieren.

Korrelation

Die Fähigkeit zur Verunreinigung durch die Verwendung statistischer Blockchainanalyse.

Gebühren

Ein impliziter Transfer an einen Miner.

Fork

Ein Abweichen der Konsensregeln.

Genesis

Der erste Block aller Zweige eines Coins.

Gültigkeit

Konformität zu Konsensregeln.

Grind

Ein Werkzeug, das Hashing durchführt.

Grinder

Eine Person, die einen Grind betreibt.

Halving

Eine Halbierung der Subvention.

Händler

Eine Person, die Einheiten im Tausch akzeptiert. Benutzer ist eine übliche Bezeichnung dafür.

Hard-Fork

Ein Fork, der eine Spaltung impliziert. Ausweitung der Menge möglicher gültiger Blöcke.

Hash

Eine atomare Berechnung, um die Validität eines Kandidaten nachzuweisen.

Hash-Power

Ein Bruchteil der Hash-Rate aller Minen.

Hash-Power-Mehrheit

Eine Untermenge von Minern mit ausreichend Hash-Power, um einen anhaltenden Angriff auszuführen. 51 % ist eine allgemeine Annäherung an eine ausreichende Leistung.

Hash-Rate

Die Rate des Hashings.

Horten

Zum Zwecke späterer Nutzung besitzen.

Identität

Die Mittel, um Kommunikation mit einer Person zu verknüpfen.

Implementierung

Ein bestimmtes Werkzeugset.

Inflation

Die Erhöhung des Angebots als Folge von Subvention. Eine Geldinflation, nicht zu verwechseln mit Preisinflation.

Kartellierung (engl. Pooling)

Die Tendenz hin zu wenigen Minen, einschließlich der Konsolidierung durch Relays.

Kreditvergabe

Der Handel zwischen Zeit ohne Einheiten und Eigentum mit größerem Nutzen. Ein anderes Wort dafür lautet Investieren.

Latenz

Die in der Kommunikation inhärente Verzögerung.

Layering

Handel in Form einer Sequenz unbestätigter Transaktionen, die durch beide Seiten abgerechnet werden kann.

Locktime

Ein Ausdruck der frühestmöglichen Gültigkeit einer Transaktion

Maschine

Ein System, das Anweisungen befolgt.

Nutzen

Die Nützlichkeit eines bestimmten Eigentums für eine Person.

Markt

Der Handel mit bestimmtem Eigentum.

Mittlere vergangene Zeit

Ein Durchschnitt der vorhergehenden Block-Zeitstempel.

Mine

Ein Werkzeug, das Arbeit verrichtet.

Miner

Eine Person, die eine Mine betreibt.

Macht

Die relative Ebene der Kontrolle einer Person über die Blockchain oder den Coin.

Nachweis (Proof)

Gültiger Beweis.

Node

Ein Werkzeug zur Validierung.

Offensichtliche Hash-Power

Ein Bruchteil von Blöcken in einem Blockchain-Segment. Öffentliche Schätzungen der spezifischen Hash-Power von Minern basieren darauf.

Operation

Eine atomare Absichtserklärung.

Optimierung

Eine Änderung an den Werkzeugen, die die Kosten des Mine reduziert.

Organisation

Eine Benachrichtigung, die der Blockchain einen Block hinzufügt.

Partition

Das Unvermögen bestimmter Nodes zu Kommunizieren.

Partitionierung

Die Tendenz hin zu persistenten Partitionen.

Peer-to-Peer

Ein symmetrisches Protokoll.

Periode

Die durchschnittliche Zeit zwischen Organisationen.

Person

Ein Entscheidungsträger.

Punkt

Eine Referenz auf einen Ausgang oder Eingang.

Politisch

Bezogen auf die Handlung von Staaten.

Preis

Eine durchschnittliche oder spontane Tauschrate.

Preisinflation

Der Anstieg des Preises über die Zeit.

Profit

Eine Rendite auf eine Investition, die über dem marktüblichen Zinssatz liegt.

Proof-of-Memory

Probabilistischer Nachweis eines Anteils des nutzbaren Rechenspeichers (PoM).

Proof-of-Stake

Kryptografischer Nachweis eines Anteils des Eigentums (PoS).

Proof-of-Work

Probabilistischer Nachweis eines Anteils der erbrachten Arbeit (PoW).

Protokoll

Eine Menge von Konventionen zur Kommunikation.

Regel

Eine Untermenge der Konsensregeln.

Reife

Die Tiefe ab der ein Coinbase-Ausgang transferierbar wird.

Relay

Ein Werkzeug, das neue Blöcke verbreitet.

Relayer

Eine Person, die ein Relay betreibt.

Reorganisation

Eine Benachrichtigung , die den Anschluss eines schwachen Zweiges an die Blockchain vorantreibt. Reorg ist eine Abkürzung dafür.

Skript

Eine Menge von Operationen, die den Transfer autorisieren.

Schwach

Ein Zweig mit weniger kumulativem Nachweis als ein anderer. Waise (Orphan) ist eine Fehlbezeichnung dafür.

Schwierigkeit

Die Ebene an Nachweis zur Bestätigung der Gültigkeit.

Segment

Eine zusammenhängende Teilmenge eines Zweiges.

Signal

Der Hinweis eines Miners über die Absicht eine neue Regel durchzusetzen, übermittelt durch Blockdaten.

Soft-Fork

Ein Fork, der eine Spaltung impliziert, sofern er nicht durch die Mehrheit der Hash-Power durchgesetzt wurde. Verkleinerung der Menge potenziell gültiger Blöcke.

Spaltung

Eine Zweiteilung eines Coins.

Spekulieren

Besitzen in der Erwartung einer Preissteigerung. Außerdem Kreditvergabe in Erwartung eines Preisrückgangs.

Staat

Eine Menge von Personen, die Aggression anstelle von Handel nutzen. Operiert in der Regel innerhalb geografischer Grenzen.

Stark

Ein Zweig mit mehr kumulativem Nachweis gegenüber einem anderen.

Staub

Eine unzureichende Anzahl von Einheiten für den Transfer über einen Ausgang. BTC-Konsens-Regeln verbieten die Übertragung von weniger als seiner Einheit.

Stillstand

Das Ausbleiben der Steigerung der Blockhöhe über die Zeit.

Subvention

Die Ausgabe neuer Einheiten an einen Miner.

Tausch

Der Tauschhandel von Einheiten gegen anderes Eigentum.

Tauschhandel

Ein freiwilliger Austausch von Eigentum zwischen zwei Personen.

Tiefe

Ein Block mehr als die Anzahl an Blöcken nach einer Bestätigung.

Transaktion

Ein gültiger Eintrag eines Transfers.

Transaktions-Pool

Die Menge an unbestätigten Transaktionen. Speicher-Pool (mempool) ist eine unzutreffende Bezeichnung dafür.

Transfer

Der Wechsel der Kontrolle über bestimmte Einheiten.

Treuhänder

Eine Person , die aufgrund einer Vereinbarung über das Eigentum eines anderen verfügt. Verwahrer (Custodian) ist ein anderer Begriff dafür.

Unbestätigt

Eine Transaktion, die nicht in einem Block der Blockchain existiert.

Validierung

Der Prozess der Bestimmung der Gültigkeit.

Varianz

Die wechselnde Häufigkeit eine Belohnung zu erhalten.

Variation

Unterschiede in den Kosten für die Produktionsmittel des Minings.

Verlust

Misserfolg einer Kreditvergabe, den marktüblichen Zinssatz zu erwirtschaften.

Vertrag

Ein Skript, das Transfer-Bedingungen ausdrückt. Public-Key-Script ist ein Anachronismus dafür.

Verunreinigung

Bestimmung der Besitzverhältnisse.

Verzerrung

Marktaggression, die Miningkosten verzerrt.

Volatilität

Schwankung des Preises über die Zeit.

Zurückhalten

Das absichtliche Verzögern von Bekanntmachungen.

Vorheriger Ausgang

Der Ausgang, auf den sich ein Eingang bezieht.

Wallet

Ein Werkzeug, das Transaktionen erstellt.

Werkzeug

Ein Satz von Maschinenbefehlen.

Wert

Die Präferenz einer Person für ein bestimmtes Gut gegenüber einem anderen.

Wirtschaft

Die Menge aller Händler.

Wirtschaftskraft

Ein Bruchteil allen zum Tausch angebotenen Eigentums.

Zeitstempel

Die Bekanntgabe der Zeit der Block-Produktion.

Zensur

Subjektive Bestätigung.

Zentralisierung

Die Tendenz hin zu wenigen Händlern. Händler kontrollieren die Validierung unmittelbar. Kann sich ebenso auf Pooling beziehen.

Zins

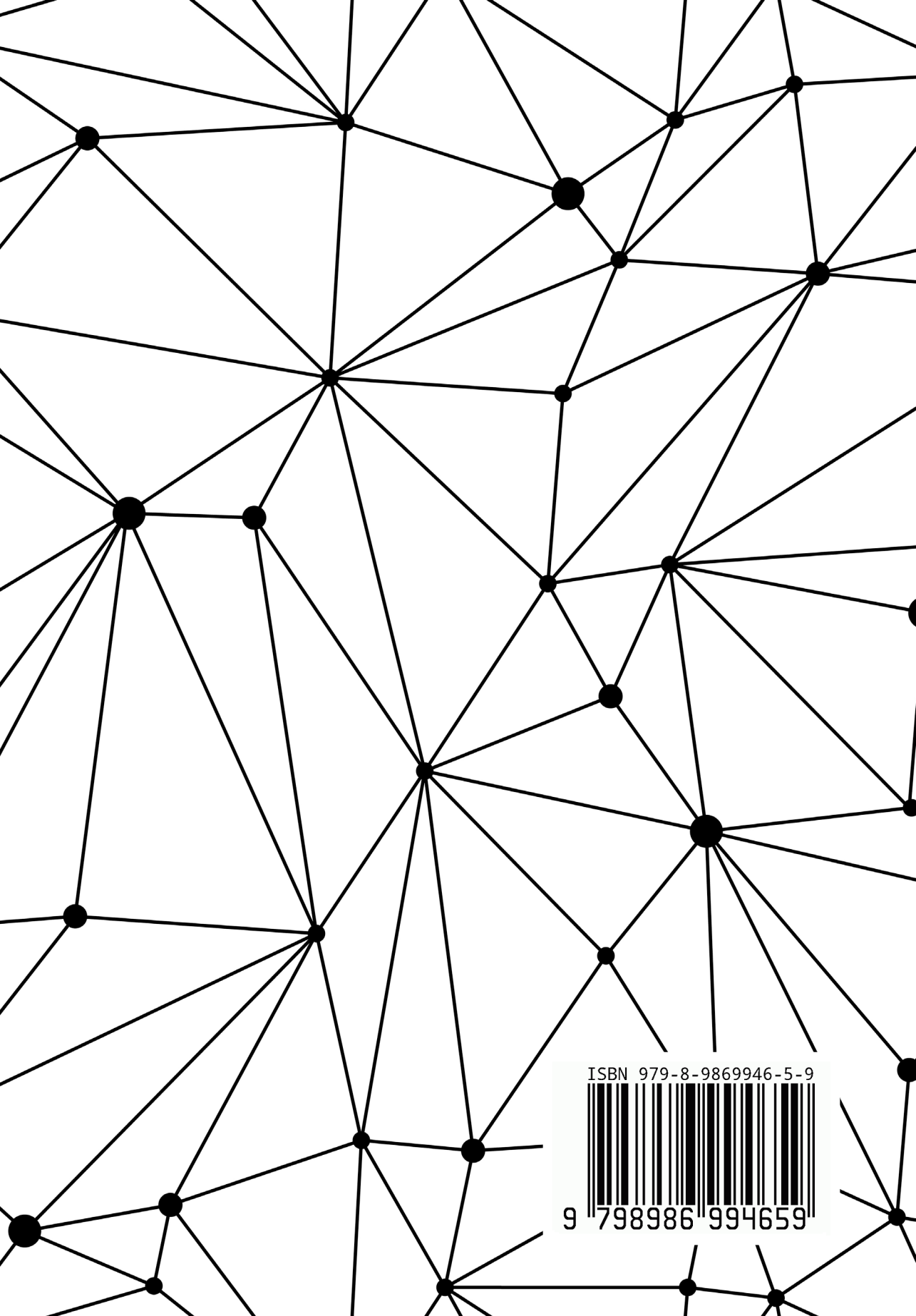
Die Rate der Erhöhung des Nutzens durch Kreditvergabe.

Zwang

Der Gebrauch von Aggression, um eine Aktivierung zu erzwingen.

Zweig

Eine gültige Sequenz von Blöcken.


ISBN 979-8-9869946-5-9