LI-Briefing

Blockchain und Kryptowährungen – ein Weg zur Freiheit?

OLIVIER KESSLER * • Dezember 2017

Für die einen sind Kryptowährungen und die Blockchain-Technologie ein Hype. Andere hingegen erkennen darin revolutionäres Umwälzungspotenzial für Politik, Wirtschaft und Gesellschaft. Revolutionen – verstanden als jähe, tiefgreifende Umbrüche – waren vielfach die Folge technologischer Neuerungen. Die Aufklärung etwa wäre ohne die Erfindung des Buchdrucks nicht denkbar gewesen. Erst die moderne kohlebetriebene Dampfmaschine und der Bau von Eisenbahnen ermöglichten die Erste Industrielle Revolution (1760-1840), während die Zweite Industrielle Revolution – die im späten 19. Jahrhundert begann und bis ins frühe 20. Jahrhundert andauerte – der Erfindung des Fliessbandes und des Verbrennungsmotors, sowie der Nutzung der Elektrizität und des Erdöls zu verdanken war. Die in den 1960er Jahren beginnende Dritte Industrielle Revolution geht zurück auf die Entwicklung von Halbleitern, Grossrechnern (1960er Jahre), Personalcomputern (1970er und 1980er Jahre) und des Internets (1990er Jahre). Es gibt nun Stimmen, die in der Erfindung der Blockchain-Technologie eine weitere entscheidende technologische Neuerung sehen, welche sie mit der Erfindung der Dampfmaschine, des Verbrennungsmotors oder des Internets vergleichen. Die damit längerfristig erwarteten Umwälzungen werden deshalb manchmal als «Blockchain-Revolution» bezeichnet.[1]

Die Blockchain-Technologie wird in erster Linie mit Kryptowährungen in Verbindung gebracht. Diese sind auch in der Schweiz vermehrt ins Rampenlicht gerückt. Aufgrund ihrer relativ günstigen Gesetzgebung ist die Schweiz attraktiv für Unternehmen, die im Bereich der «Cryptofinance» operieren. Viele von ihnen haben sich im sogenannten «Crypto Valley» im Kanton Zug niedergelassen. Die starken Kursgewinne und die Volatilität von Kryptowährungen haben zudem das Interesse von Investoren und Spekulanten geweckt. Ende 2017 soll hierzulande der weltweit erste regulierte Investmentfonds für Kryptowährungen starten.[2] Im September 2017 hat die Eidgenössische Finanzmarktaufsicht FINMA zudem angekündigt, dass sie manche in

* Der Autor, M.A. HSG in International Affairs and Governance, ist Vizedirektor am Liberalen Institut.

[1] Vgl. dazu etwa: Don Tapscott und Alex Tapscott (2016). *Die Blockchain Revolution*. Kulmbach: Börsenmedien AG.

[2] Werner Grundlehner (14. Juni 2017). *Im Rennen um den ersten Krypto-Fonds*. https://www.nzz.ch/finanzen/fonds/ein-fonds-fuer-bitcoin-co-im-rennen-um-den-ersten-krypto-fonds-ld.1300587

der Schweiz abgehaltene «Initial Coin Offerings» (ICOs) genauer unter die Lupe nehmen möchte.[3] Kurz zuvor hatte die *Crypto Valley Association* ihren Support für vorsichtige Regulierungen und einen «Code of Conduct» im Bereich dieser ICOs angekündigt.[4]

Es tut sich also einiges an der Front der Blockchain-Technologie und der Kryptowährungen und es ist an der Zeit, eine aktuelle Einschätzung und Einordnung aus politökonomischer Sicht vorzunehmen. Dafür ist es einerseits unvermeidlich, zu den Anfängen der Blockchain-Technologie zurückzukehren und zu fragen, zur Lösung welcher Probleme diese entwickelt wurde und ob sie dafür geeignet ist, diese Probleme auch tatsächlich nachhaltig zu lösen. Weiter soll beleuchtet werden, was die Blockchain-Technologie für die individuelle Freiheit bedeutet. Welche Potentiale birgt sie für überfällige Entstaatlichungsmassnahmen? Hilft sie dabei, den Bürgern mehr Kontrolle über ihr eigenes Leben zurückzugeben oder ist sie unter dem aktuell vorherrschenden sozialdemokratischen Zeitgeist vielleicht sogar eine Gefahr für Freiheit, Verantwortung und Privatsphäre der Menschen?

Grundproblematik des staatlichen Geldsystems

Wer den Nutzen der Blockchain-Technologie im Währungsbereich verstehen will, kommt nicht darum herum, sich einige grundsätzliche Fragen zum heutigen Geldsystem zu stellen. Denn Kryptowährungen sind als Reaktion auf einige problematische Umstände ebendieses Geldsystems entstanden. Welche Herausforderung wollte der Erfinder (oder die Erfinder)[5] mit dem Pseudonym Satoshi Nakamoto lösen, als er an der Blockchain-Technologie tüftelte?

Er erkannte das staatliche Geldmonopol als eines der zentralen Probleme der heutigen Zeit, was auf den ersten Blick nicht offensichtlich erscheinen mag, zumal die meisten Volkswirtschaften auch mit oder trotz des staatlichen Geldmonopols funktionieren und real wachsen. Die staatliche Herrschaft über das Geld impliziert, dass es ein gesetzliches Zahlungsmittel und einen entsprechenden Annahmezwang für Gläubiger gibt, wenn jemand seine Schulden mit dem vom Staat festgelegten Zahlungsmittel begleichen möchte. Zugleich definiert der Staat, wer neues Geld ausgeben darf, und überträgt diesen Akteuren die Macht über die Festlegung des Geldangebots. In den meisten Ländern handelt es sich um ein sogenanntes «fraktionales Reservesystem», in welchem die Zentralbank für die Schöpfung von Bargeld verantwortlich ist, während staatlich lizenzierte Geschäftsbanken neues Giralgeld – also elektronische

[3] FINMA (29. September 2017). *FINMA trifft Abklärungen bei ICOs*: https://www.finma.ch/de/news/2017/09/20170929-mm-ico/

[4] Crypto Valley Association (7. September 2017). *Crypto Valley Association Comes Out in Support for Careful ICO Regulation; Announces ICO Code of Conduct*: https://cryptovalley.swiss/crypto-valley-association-comes-support-careful-ico-regulation-announces-ico-code-conduct/

[5] Ob hinter dem Erfinder der Blockchain-Technologie, der mit dem Pseudonym Satoshi Nakamoto auftrat, eine Einzelperson oder eine Gruppe steckt, ist bis heute unbekannt. Nachfolgend gehen wir der Einfachheit halber davon aus, dass es sich um eine Einzelperson gehandelt hat.

Sichtguthaben – via Kreditvergabe ausgeben. Letzteres macht mittlerweile vielerorts über 90 Prozent der gesamten Geldmenge aus.

In der Weltgeschichte wimmelt es von Ereignissen, in welchen das staatliche Geldmonopol auf Kosten der Bürger massiv missbraucht worden ist. Dabei braucht man gar nicht zwingend an jüngste Extremereignisse wie die Zypern-Krise zu denken, als Guthaben der Bankkunden eingefroren und via «Bail-in» teilenteignet wurden. Der Machtmissbrauch im Bereich des Geldwesens ist omnipräsent und manifestiert sich beispielsweise in der dauerhaft inflationären Geldpolitik, neuerdings mit Negativzinsen und massiver Geldschwemme, mit welcher die Ersparnisse der Bürger schleichend oder galoppierend entwertet werden – auch wenn dies durch die offizielle Inflationsmessung vertuscht wird.[6] Auch verhindert die staatliche Geldpolitik dringend benötigte Korrekturen von Fehlinvestitionen, die für die Gesundheit einer Volkswirtschaft essentiell sind, indem der Geldhahn in sich anbahnenden Korrekturphasen einfach noch weiter aufgedreht wird. So werden unrentable Firmen und Branchen auf Kosten der Allgemeinheit unter dem Deckmantel der «Krisenbekämpfung» und der «Ankurbelung der Wirtschaft» subventioniert. Die vom Staat selbst geschaffenen Probleme dienen ihm als Legitimation, immer weitere fragwürdige Eingriffe in marktwirtschaftliche Prozesse vorzunehmen, was letztlich zu einer laufend grösseren Entfremdung eines Teils der Produktion von den tatsächlichen Bedürfnissen der Bürger führt.

Die Probleme einer Gesellschaft, in welcher der Staat die Herrschaft über das Geld innehat, sind grundsätzlich dieselben, unter welchen jeder planwirtschaftlich organisierte Gesellschaftsbereich leidet: [1] Es herrscht ein Mangel an Information und eine Anmassung von Wissen beim Zentralplaner (im Gegensatz zur Nutzbarmachung der dezentralen «Weisheit der Vielen» in einer freien Marktwirtschaft, in welcher Entscheidungen nach dem ökonomischen Kalkül gefällt werden). [2] Marktpreise werden durch politisch befohlene Preise (im Fall der Zentralbanken die Leitzinsen) ersetzt. Dies führt in der Folge zu einem Wegfall von Knappheitssignalen in Form von steigenden Preisen bei sich abzeichnender Aufzehrung eines Gutes. Fehlen solche Signale, nimmt die Verschwendung knapper Ressourcen zu (Stichwort: Fehlinvestitionen). [3] Es besteht die Gefahr von Machtmissbrauch beim Zentralplaner (etwa in Form der Monetisierung staatlicher Schulden). [4] Eigentumsrechte werden verletzt (Ersparnisse verlieren beispielsweise an Wert bei einer expansiven Geldpolitik). [5] Individuen werden in ihrer Möglichkeit eingeschränkt, gemäss ihren eigenen Präferenzen und Bedürfnissen zu wählen (sie dürfen beispielsweise nicht darauf bestehen, jenes Geld an Zahlung zu nehmen, welches sie bevorzugen).

Satoshi Nakamoto hatte diese Probleme des staatlichen Geldsystems erkannt. Am 11. Februar 2009 – inmitten der ausgebrochenen Finanzkrise – schrieb er in einem Forum für Entwickler: «Das Kernproblem der herkömmlichen Währungen ist, dass sie Vertrauen brauchen, um ihre Funktion erfüllen zu können. Die Menschen müssen der Zentralbank vertrauen, dass sie die Währung nicht entwertet, aber in der Geschichte

[6] Vgl. dazu Jörg Guido Hülsmann (2013). *Krise der Inflationskultur*. München: FBV. S. 138-145.

des Fiatgelds wimmelt es von Fällen, in denen dieses Vertrauen missbraucht wurde. Wir müssen den Banken vertrauen, dass sie unser Geld aufbewahren und es elektronisch überweisen, aber sie verleihen es immer wieder mit einem Bruchteil an Deckung, und es entstehen Kreditblasen.» In einem anderen Beitrag schrieb er: «Entziehen wir uns dem unkontrollierbaren Inflationsrisiko zentral gesteuerter Währungen!»[7] Michael Casey und Paul Vigna, Autoren des Buchs *Cryptocurrency*, beschreiben das Projekt Nakamotos mit Hinweis auf die dunklen Tage der damaligen Finanzkrise treffend als «Antithese des Systems, das das zentrale Problem in diesem historischen Augenblick war.»[8]

Staatliches Geldsystem als Ursache von Finanz- und Wirtschaftskrisen

Es muss allerdings betont werden, dass die staatliche Herrschaft über das Geld und geldpolitische Interventionen nicht nur in diesem einen historischen Zeitpunkt, sondern grundsätzlich eines der zentralen ökonomischen Probleme darstellen, weil dadurch dringend benötigte Korrekturen aufgeschoben werden und einer Blasenbildung Vorschub geleistet wird.

Heute vertreten viele Ökonomen die Auffassung, dass Geld zwingend vom Staat kontrolliert werden müsse. Sie ignorieren damit jedoch die Erkenntnisse der Ökonomen, die in der freiheitlichen Tradition der Österreichischen Schule der Nationalökonomie stehen. Carl Menger, der Begründer der Österreichischen Schule, legte 1871 dar, dass sich Geld als Tauschgut in einem Entdeckungsverfahren der Menschen herausgebildet haben muss und dafür keinerlei Staatseingriffe nötig waren.[9] In der Vergangenheit nahmen verschiedene Güter die Funktion des allgemein akzeptierten Tauschmittels an. Von Salz, Korn und Tee über Glasperlen, Nägel und Tabak bis hin zu Kupfer, Silber und Gold – ja selbst Papierscheine, die ein Anrecht auf einen bestimmten Anteil an Silber oder Gold darstellten – galten zu unterschiedlichen Zeiten und verschiedenen Orten diverse Güter als Geld.[10] Jörg Guido Hülsmann nennt diese durch freiwillige Übereinkunft zustande gekommene Tauschmittel «natürliches Geld».[11] Davon unterscheidet sich das heutige «Zwangsgeld» in Form von Papierscheinen und Giralgeld, welches sich durch folgende Merkmale auszeichnet: «(1) die Monopolstellung eines staatlich bevorzugten Geldproduzenten, z.B. einer Bank; (2) der Annahmezwang des vom Monopolisten emittierten Papiergeldes bzw. elektronischen Geldes; (3) ungeahndete Zahlungseinstellungen des Monopolisten».[12]

Frank Schäffler und Norbert Tofall weisen darauf hin, dass unser heutiges Zwangsgeld «schlechtes Geld» sei, «weil es von den Zentralbanken und auch von den

[7] Michael Casey und Paul Vigna (2015). *Cryptocurrency – Wie virtuelles Geld unsere Gesellschaft verändert*. Berlin: Ullstein. S. 94.
[8] Ebd S. 95.
[9] Carl Menger (2007). *Principles of Economics*. Auburn: Ludwig von Mises Institute. S. 257-262.
[10] Murray N. Rothbard (2005). *Das Schein-Geld-System – Wie der Staat unser Geld zerstört* (2. Aufl.). Gräfelfing: Resch. S. 18.
[11] Jörg Guido Hülsmann (2007). *Die Ethik der Geldproduktion.* Waltrop und Leipzig: Manuscriptum Verlagsbuchhandlung. S. 38-39.
[12] Jörg Guido Hülsmann (2011). Ethische Probleme der Währungspolitik. In Peter Altmiks (Hrsg.). *Im Schatten der Finanzkrise – Muss das staatliche Zentralbankwesen abgeschafft werden?* (S. 13-34). München: Olzog.

Geschäftsbanken, die vom Staat zum Zwecke der Geld- und Kreditschöpfung aus dem Nichts mit dem Teilreserveprivileg ausgestattet sind, in beliebiger Höhe vermehrt werden kann».[13] Ein weiterer problematischer Aspekt ist die Möglichkeit des Geldmonopolisten, den Zins festzulegen. Bereits Ludwig von Mises leitete 1912 in seinem bahnbrechenden Klassiker *Theorie des Geldes und der Umlaufmittel* her, weshalb die politische Festlegung des Zinses zu Blasenbildungen und wiederkehrenden Finanz- und Wirtschaftskrisen führen muss.[14] Um dies zu verstehen, soll nachfolgend zunächst die Koordination der gesamtwirtschaftlichen Ersparnissen und Investitionen durch den (durch das freie Zusammenspiel von Angebot und Nachfrage entstehenden) natürlichen Zins in einem Umfeld des freien Marktes betrachtet – also ein Umfeld, in dem es keine staatlichen Interventionen gibt, wie zum Beispiel die künstliche Reduktion des Zinses durch eine Zentralbank –, und anschliessend aufgezeigt werden, weshalb die planwirtschaftlichen Eingriffe durch die Zentralbanken diese Koordination stören.

Gemäss Eugen Böhm von Bawerk wird die Spar- und Konsumneigung der Individuen durch ihre Zeitpräferenz bestimmt.[15] Eine hohe Zeitpräferenz bedeutet, dass es dem Individuum wichtiger ist, möglichst bald konsumieren zu können. Jemand mit einer geringeren Zeitpräferenz ist bereit, mit seinem Konsum noch etwas zuzuwarten, um zu einem späteren Zeitpunkt mehr konsumieren zu können. Der natürliche Zins ist hauptsächlich das Abbild dieser Zeitpräferenzen. Jemand, der nur ungern auf den sofortigen Konsum verzichten will, wird für den Verzicht des Konsums eine hohe Kompensation einfordern. Person A mit einer hohen Zeitpräferenz würde vielleicht nur dann auf den sofortigen Verzehr von 100 Trauben verzichten, wenn sie dafür zu einem späteren Zeitpunkt 115 Trauben bekommt. Hingegen werden jene, die eine niedrigere Zeitpräferenz aufweisen, eine relativ geringe Ausgleichszahlung verlangen. Person B könnte allenfalls schon auf den sofortigen Verzehr von 100 Trauben verzichten, wenn sie dafür später 103 Trauben bekommt. Diese verlangten Kompensationszahlungen entsprechen vereinfacht gesagt der Höhe des Zinses. Person A will im obigen Beispiel also einen Zins von 15%, während Person B mit 3% zufrieden ist, um auf den sofortigen Konsum zu verzichten. Selbstverständlich enthalten die Zinssätze auf den natürlichen Kreditmärkten (also Kreditmärkte ohne Eingriffe durch eine Zentralbank) noch weitere Elemente, wie etwa Risikoprämien für allfällige Kredit- oder Kaufkraftverluste. Das wichtigste Element ist aber die Zeitpräferenz.[16]

Wie schafft es der natürliche Zins, Ersparnisse und Investitionen relativ harmonisch aufeinander abzustimmen? Angenommen, die Zeitpräferenzen der Individuen in einer Gesellschaft seien tendenziell eher niedrig. Relativ viele Menschen sparen und legen ihre Ersparnisse an. Sie drücken dadurch den Zinssatz herunter, weil das

[13] Frank Schäffler und Norbert F. Tofall (2010). Währungswettbewerb als Evolutionsverfahren. In Peter Altmicks (Hrsg.) *Im Schatten der Finanzkrise – Muss das staatliche Zentralbankwesen abgeschafft werden?* (S. 135-155). München: Olzog.
[14] Ludwig von Mises (1912). *Theorie des Geldes und der Umlaufmittel*. München: Duncker und Humblot.
[15] Eugen Böhm von Bawerk [1891] (1930). *The Positive Theory of Capital* (W. Smart, Übers.). New York: G. E. Stechert und Co.. S. 285-424.
[16] Detlev S. Schlichter (2013). *Das Ende des Scheins – Warum auch unser Papiergeldsystem zusammenbricht*. Weinheim: Wiley. S. 142.

Angebot der für Investitionen zur Verfügung stehenden Ersparnisse dadurch ausgeweitet wird. Der niedrige Zinssatz wiederum signalisiert den Investoren: Es gibt verhältnismässig günstige Kredite. Mehr Unternehmer werden deshalb Kredite aufnehmen, da ihre geplanten Projekte nun rentabel erscheinen. Durch die (durch Ersparnisse verfügbar gemachten) Kredite, können Unternehmer heute investieren, damit sie die Konsumwünsche von morgen befriedigen können. Die Bürger ihrerseits können sich diese künftig verfügbaren Produkte durch ihre Ersparnisse leisten. Die Präferenzen der Menschen werden durch die Koordination des natürlichen Zinses in einer freien Marktwirtschaft folglich aufeinander abgestimmt.

Warum gerät diese gesamtwirtschaftliche Koordination durch staatliche Interventionen im Geldwesen durcheinander? Die Zeitpräferenz hat nicht nur Einfluss auf den Zinssatz. Die Höhe des existierenden Zinssatzes hat auch Einfluss auf die Zeitpräferenz der Individuen.[17] Diese Tatsache ermöglicht einer Zentralbank eine gewisse gesellschaftliche und wirtschaftliche Steuerung. So erhöht ein künstlich heruntergedrückter Zinssatz die Zeitpräferenz der Menschen, was bedeutet, dass dem Gegenwartskonsum tendenziell ein grösserer Wert eingeräumt wird als bei höherem Zins. Bei einem höheren Zinssatz würde es sich eher lohnen, Geldeinkommen zu sparen als direkt zu konsumieren, da durch den höheren Zins ein grösserer Ertrag in der Zukunft erwartet wird. Durch einen künstlich niedrigen Zins nimmt die Konsumneigung in der Tendenz zu. Obwohl nun wegen des geringen Zinssatzes weniger Ersparnisse für Investitionen zur Verfügung stehen, ermöglicht es die Kreditgeldschöpfung der Zentral- und Geschäftsbanken, dass trotzdem genügend Mittel für Investitionen verfügbar gemacht werden und diese aufgrund billiger Zinsen auch in Anspruch genommen werden. Es wird gegenwärtig mehr konsumiert, weniger gespart und trotzdem mehr investiert. Die getätigten Investitionen (ohne das Vorhandensein der nötigen Ersparnisse) führen in der Folge zu einem Scheinwachstum, das in einer Wirtschaftskrise enden muss, wenn die Fehlinvestitionen offensichtlich werden. Die Unternehmen bleiben auf ihren Produkten sitzen und gehen Konkurs – die Blase platzt.

In dieser Phase eilt normalerweise die Zentralbank den gescheiterten Unternehmen zu Hilfe, indem sie Kredite durch das Heruntermanipulieren der Zinsen weiter verbilligt. Damit verhindert sie den dringend benötigten Anpassungsprozess der Volkswirtschaft, dank welchem knappe Ressourcen wieder jenen Orten zugeführt werden, an welchen sie am dringendsten gebraucht werden. So macht sich die Zentralbank der Ressourcenverschwendung im grossen Stil schuldig und heizt bereits wieder die nächste – noch grössere – Blasenbildung an. Ein Teufelskreis, in welche uns die staatliche Geldpolitik hineinmanövriert hat. Jedes Mittel scheint recht zu sein: Die geldpolitischen Zentralplaner schrecken mittlerweile nicht einmal vor riskanten Experimenten wie Negativzinsen und «Quantitative Easing» zurück. Immer mehr Bürger machen sich deshalb Sorgen über die Zukunft des Geldes und über die Folgen der längerfristig wohl unvermeidlichen Bereinigungsprozesse.

[17] Roland Baader (2010). *Geldsozialismus – Die wirklichen Ursachen der neuen globalen Depression*. Gräfelfing: Resch. S. 86.

Die Entstehung der Blockchain-Technologie

Unter anderem aus diesen Gründen machten sich einige Tüftler daran, Alternativen zum staatlichen Geld zu schaffen, die nicht mehr der Manipulation der Behörden ausgesetzt sind. Satoshi Nakamoto war mit der Erfindung der Blockchain-Technologie keinesfalls der erste, der einen solchen Versuch unternommen hatte. Die erste Blockchain-basierte Kryptowährung – der Bitcoin – hatte einige Vorläufer wie etwa «Digicash», «B-money» und «Hashcash».[18] Bereits frühere Softwareprotokolle erlaubten es den Nutzern, durch kryptografische Verschlüsselungsverfahren auf sichere Weise Überweisungen zu tätigen. Auch stellten sie eine Reihe nicht zu brechender Regeln auf, mit denen sich ein dezentrales Computernetzwerk koordinieren sollte, dem sich jeder anschliessen kann, wenn er die entsprechende Software herunterlädt.

Die Vorgänger von Bitcoin sind jedoch allesamt gescheitert – hauptsächlich, weil sie das Problem der doppelten Ausgabe (also das mehrfache Ausgeben derselben digitalen Geldeinheit) nicht zu lösen vermochten. Zudem war es auch schwierig, sich ohne zentrale Autorität auf einen Konsens des Grundbuchs zu einigen. Folglich ergaben sich wieder dieselben Vertrauensprobleme aufgrund einer zentralen Institution, die das Grundbuch verwaltete.

Trotz des Scheiterns aller Versuche, dem staatlichen Geld eine ernstzunehmende digitale Alternativwährung gegenüberzustellen, war Nakamoto davon überzeugt, dass sein System überleben würde. Denn ihm war bewusst, dass dieses bahnbrechende Neuerungen beinhaltet, welche die vorgängigen Probleme digitaler Währungen beseitigt: Einerseits das universelle, öffentlich einsehbare Grundbuch, welches dazu dient, dass jeder Teilnehmer überprüfen kann, ob Transaktionen gültig sind; andererseits eine neuartige Anreizstruktur, welche die Netzwerkteilnehmer dazu motiviert, stets einen Konsens über den aktuellen Stand des Grundbuchs zu erzielen – nämlich indem jene, die sich daran beteiligen, das Grundbuch aktuell zu halten, monetär durch neuausgegebene digitale Münzen und Transaktionsgebühren belohnt werden. Indem jeweils derjenige Netzwerkteilnehmer einen neuen Block (der unter anderem Informationen zu den gültigen Transaktionen und einen Zeitstempel enthält) an die bestehende Blockkette anhängen darf, der es zuerst schafft, eine mathematisch anspruchsvolle «Hashing»-Rechenaufgabe zu lösen (dieses Verfahren wird auch «Proof-of-Work» genannt), die Lösung aber von den anderen Teilnehmern einfach überprüft werden kann, wird rund alle 10 Minuten im Netzwerk ein Konsens über das Grundbuch hergestellt.[19] Bei anderen Kryptowährungen geht diese Konsensfindung mittlerweile schneller.

In der «Blockkette» werden Transaktionen in chronologisch geordneten Blöcken gespeichert, nachdem sie von den Netzwerkteilnehmern auf ihre Gültigkeit überprüft, mit dem historischen Grundbuch abgeglichen und bestätigt worden sind. Durch diese Verkettung von Blöcken wird ermöglicht, dezentral einen Konsens über die

[18] Vgl. dazu: Michael Casey und Paul Vigna (2015). *Cryptocurrency – Wie virtuelles Geld unsere Gesellschaft verändert*. Berlin: Ullstein. S. 67-101.
[19] Für technisch ausführlichere Beschreibungen der Funktionsweise von Bitcoin siehe: Andreas M. Antonopoulos (2017). *Mastering Bitcoin – Programming the Open Blockchain* (2. Aufl.). Sebastopol: O'Reilly.

Transaktionshistorie zu erzielen. Diese wichtige Neuerung vermochte das Problem der digitalen Geldfälschung zu lösen, weil Transaktionen vom Netzwerk als ungültig erkannt werden, wenn versucht wird, dieselbe Geldeinheit zweimal auszugeben und weil Manipulationsversuche an der bisherigen Blockkette aufgrund von «Hashing»-Verknüpfungen der Blöcke sofort auffliegen.

Auch wurde durch die Dezentralisierung der Grundbuchverwaltung ein wesentliches Problem des heutigen Geldsystems gelöst: Es braucht theoretisch keine zentrale Institution mehr, welche das Vertrauen durch seine Reputation herstellt. Die Blockchain-Technologie wird folglich auch als «vertrauensloses Netzwerk» bezeichnet. Diese Bezeichnung ist allerdings nur teilweise zutreffend: Vielmehr stecken die Netzwerkteilnehmer ihr Vertrauen neu in von Menschen geschaffene Programmiercodes, die – wie der Mensch selbst – ebenfalls fehleranfällig sein können. Die Softwareprotokolle der meisten Kryptowährungen sind öffentlich nach dem «open source»-Prinzip einsehbar. Das bedeutet, jeder, der etwas von der (hoch anspruchsvollen) Technologie versteht, kann das Netzwerk angreifen und testen.

Wenn Algorithmen statt Zentralbanken Geld schöpfen

Welche möglichen geldpolitischen Implikationen hat die Erfindung von Kryptowährungen? Eine wichtige Eigenschaft von Geld ist seine Knappheit. Staatliches Geld erfüllt diese Eigenschaft allerdings nur solange, wie die Entscheidungsträger, welche das Geldangebot kontrollieren und in welche die Bürger ihr Vertrauen setzen müssen, Disziplin walten lassen. Praktisch auf Knopfdruck können Zentral- und Geschäftsbanken zu tiefen Kosten neues Geld schöpfen und damit den Wert bisher existierender Geldeinheiten mindern, teilweise sogar drastisch, wie Erfahrungen mit der Hyperinflation gezeigt haben – etwa 1923 in der Weimarer Republik, 2008 in Simbabwe oder aktuell in Venezuela. Vorausgesetzt, der entsprechende Programmiercode einer Kryptowährung erweist sich als robust, würde dies bedeuten, dass die Menschen in Geldfragen (und nicht nur dort, wie wir später noch sehen werden) nicht mehr zwingend ihr Vertrauen in Vermittler stecken müssen, sondern sich auf vorhersehbare, öffentlich einsehbare Algorithmen verlassen könnten.

Nach welchem Prinzip funktioniert bei Kryptowährungen die Geldschöpfung? Bei sogenannten «Proof-of-Work»-Währungen wie beispielsweise Bitcoin erhält jener Netzwerkteilnehmer – der sogenannte «Miner» –, der es geschafft hat, jeweils als erstes eine anspruchsvolle Rechenaufgabe zu lösen und einen weiteren gültigen Block an die Blockkette anzuhängen, eine bestimmte, im Zeitverlauf abnehmende Menge neu geschöpfter digitaler Münzen – quasi als Entschädigung für die Rechenleistung, welche er dem Netzwerk zur Verfügung gestellt hat. Bei Bitcoin etwa wird die Belohnung alle 210 000 Blöcke – was ungefähr einer Zeitdauer von vier Jahren entspricht – halbiert. Durch diese periodische Abnahme des Geldmengenwachstums, das voraus-

sichtlich ab dem Jahr 2140 bei null liegen wird, wird die Geldmenge bei rund 21 Millionen Einheiten gedeckelt.[20] Das bedeutet – mindestens im Ansatz – eine grössere Vorhersehbarkeit des künftigen Werts der Währung (weil nur noch die entsprechende Geldnachfrage variieren kann, das Angebot aber im Vorhinein definiert ist), sowie eine Beseitigung von unkalkulierbarem Inflationsrisiko, indem die Möglichkeit ausgeschlossen wird, dass Zentralbanken den Wert der Währung durch eigens beschlossene Flutung der Märkte mit neu geschaffenem Geld mindern oder zerstören.

Manche Ökonomen – insbesondere jene, die in der Tradition des Monetarismus und des Keynesianismus stehen – warnen üblicherweise in Anbetracht einer Deckelung der Geldmenge vor deflationären Tendenzen. Bei steigender Produktivität (oder einem steigenden Güter- und Dienstleistungsangebot) würde bei einer fixen Geldmenge der Wert der einzelnen Geldeinheiten steigen, weil damit mehr Güter und Dienstleistungen erworben werden können. Solche Szenarien werden von diesen Ökonomen als volkswirtschaftlich schädlich erachtet, weil sie von der Theorie der «Deflationsspirale» ausgehen, wonach die Konsumenten mit dem Kauf gewisser Dinge angeblich immer weiter zuwarten, weil diese in Zukunft noch billiger und die Unternehmen folglich auf ihren Angeboten sitzenbleiben würden, was letztere in den Ruin treiben, Arbeitsplätze vernichten und damit zu weiteren Nachfrageausfällen führen würde.

Diese Darstellung vermag jedoch weder in der Theorie noch in der Praxis zu überzeugen: Erstens wollen Menschen tendenziell eher heute als morgen ihre Bedürfnisse befriedigen. Es macht schlichtweg keinen Sinn, ewig mit einem Kauf zuzuwarten, nur weil das Objekt des Begehrens in Zukunft allenfalls noch etwas billiger sein könnte, wenn das Produkt oder die Dienstleistung heute dazu führt, den Nutzen entscheidend zu erhöhen. Zweitens kann auch in der Praxis beobachtet werden, dass beispielsweise elektronische Geräte wie Handys oder auch Autos sich laufend verbessern, während die Preise gleichbleiben oder sogar häufig sinken. Trotzdem warten die wenigsten mit einem Kauf ewig zu. Wäre die Theorie der Deflationsspirale stichhaltig, müssten die Strassen leer sein und die Menschen würden noch nicht über Mobiltelefone verfügen. Es ist zudem ethisch problematisch, Menschen durch eine künstlich erzeugte Inflation zum Konsum anzuregen, wenn sie ihr Geld eigentlich lieber sparen und für den künftigen Konsum aufheben möchten. Bei der inflationären Geldpolitik handelt es sich folglich nicht nur um einen Angriff auf das Privateigentum, sondern auch um einen illegitimen staatlichen Eingriff in die Wahlfreiheit der Bürger, welcher weitgehend durch fehlgeleitete, vor allem keynesianische Scheinwissenschaft mit einem oberflächlichen Fokus auf den Konsum gerechtfertigt wird. Doch Wohlstand wird in erster Linie durch Ersparnisse und Investitionen erzeugt. Eine Gesellschaft kann sich schliesslich nicht «reichkonsumieren».

Ein weiterer Einwand gegen eine begrenzte Geldmenge besteht darin, dass diese zu knapp bemessen sein könnte und damit den Ansprüchen der Volkswirtschaft

[20] Vgl. dazu: Aleksander Berentsen und Fabian Schär (2017). *Bitcoin, Blockchain und Kryptoassets – Eine umfassende Einführung*. Norderstedt: BoD. S. 64.

nicht genügen würde. Geldtheoretiker der Österreichischen Schule gelangen hingegen zum Schluss, dass jede beliebige Geldmenge ausreichend sei (vorausgesetzt, sie ist im genügenden Ausmass teilbar), weil Menschen Kaufkraft nachfragten und nicht eine bestimmte Menge an Geld. Ein kontinuierliches Geldmengenwachstum sei folglich keine Voraussetzung einer funktionierenden Volkswirtschaft. Die Deflationstheorie dient in erster Linie als scheinwissenschaftliche Rechtfertigung eines verstaatlichten Geldwesens.

Bei der Ausweitung der Menge an Konsum- und Investitionsgütern kann man davon ausgehen, dass damit der gesellschaftliche Nutzen erhöht wird, da dies erwartungsgemäss zu mehr Wohlstand führt. Beim Geld ist dies jedoch anders. Geld wird nicht im wahrsten Sinne des Wortes aufgebraucht. Es ist ein Mittel, nicht Selbstzweck. Eine Erhöhung der Geldmenge hat daher mittelfristig lediglich zur Folge, dass sich die Kaufkraft der einzelnen Geldeinheiten verändert und sich dadurch die Preise anpassen. Durch eine Erhöhung der Geldmenge hebt man den gesamtgesellschaftlichen Wohlstand folglich nicht an. Vielmehr führt dies dazu, dass einige kurzfristig auf Kosten anderer reicher werden, wie der Ökonom Richard Cantillon belegte[21] und wie auch Andreas Marquart und Philipp Bagus im heutigen Kontext aufgezeigt haben.[22]

Jede Geldmenge ist also für die Erfüllung der Tauschfunktion ausreichend – vorausgesetzt sie ist beliebig teilbar. Während bei staatlichem Fiatgeld lediglich eine Stückelung auf zwei Stellen nach dem Komma möglich ist, erlauben Kryptowährungen eine Stückelung mit wesentlich mehr Stellen nach dem Komma, wobei künftig durch die Entwickler problemlos weitere Nachkommastellen hinzugefügt werden könnten. Eine solche Massnahme zur erhöhten Teilbarkeit darf jedoch nicht mit der Ausweitung der Geldmenge verwechselt werden, weil lediglich die Nachkommastellen davon betroffen sind. Folglich erachten die Ökonomen der Österreichischen Schule gedeckelte Geldmengen – wie sie bei vielen aber bei weitem nicht allen Kryptowährungen üblich sind – als grundsätzlich unproblematisch.

Kryptowährungen und der Hayek'sche Währungswettbewerb

Wettbewerb ist in einer freien Marktwirtschaft immer zu begrüssen, weil Konsumenten dadurch eine grössere Auswahl erhalten und Unternehmen sich stets um die Gunst der Kundschaft bemühen müssen, indem sie bessere und günstigere Produkte und Dienstleistungen anbieten als die Konkurrenz. Dies dient dem optimalen Umgang mit knappen Ressourcen. Beim Geld ist das nicht anders. Die Gefahren eines monopolisierten Geldmarktes sind schlechte Geldqualität und das Ignorieren von Kundenbedürfnissen. Ausserdem existiert in einem Monopol-Umfeld aufgrund fehlender Alternativen die Gefahr, dass die Nutzer des Geldes im Falle einer politischen

[21] Richard Cantillon (2001). *Essay on the Nature of Commerce in General* (H. Higgs, Übers.). New Brunswick: Transaction Publishers. (Originalwerk publiziert 1755).
[22] Andreas Marquart und Philipp Bagus (2014). *Warum andere auf Ihre Kosten immer reicher werden – und welche Rolle der Staat und unser Papiergeld dabei spielen*. München: FBV.

Katastrophe – wie etwa einer Hyperinflation – wenige oder keine Ausweichmöglichkeiten haben, um weiterhin verlässlich Güter und Geld gegeneinander zu tauschen. Aus den genannten Gründen ist der Wettbewerb zwischen verschiedenen Geldanbietern positiv zu beurteilen, selbst wenn die optimale Anzahl Währungen in einer Volkswirtschaft aus Effizienzgründen und zur Vermeidung von Transaktionskosten bei eins liegen würde. Letzteres würde allerdings eine für alle Wirtschaftsteilnehmer perfekte Währung voraussetzen, welche über keinerlei Verbesserungspotenzial mehr verfügt, das von der Konkurrenz behoben werden könnte.

1976 äusserte der Nobelpreisträger Friedrich August von Hayek in seiner Schrift über die Entstaatlichung des Geldes die Idee, die damalige Inflation durch eine freie Währungswahl zu stoppen und auch Privaten zu erlauben, eigene Währungen zu emittieren.[23] Damit stellte Hayek das herrschende Denken auf den Kopf, welches grossmehrheitlich besagte, dass Geld gesetzliches Zahlungsmittel sein müsse und nur von Staaten herausgegeben werden dürfe. In der Tat eröffnet die Entstehung von Kryptowährungen die Chance eines von Hayek geforderten Geldwettbewerbs – nicht nur mit Fiatgeld sondern auch unter Kryptowährungen selbst.

Viele Kryptowährungen, von denen es mittlerweile schon über tausend verschiedene gibt, sind lediglich Kopien oder leichte Abänderungen des Bitcoin-Protokolls ohne tatsächliche Nutzenvorteile für die Kunden. Es gibt aber durchaus valable Konkurrenten, die mit echten Neuerungen und Verbesserungen aufwarten. Dash, Monero, ZCash, Pivx und NavCoin etwa bieten eine erhöhte Privatsphäre und Anonymität. IOTA wartet mit der Beseitigung von Transaktionsgebühren und schnelleren Transaktionen auf. Auf der Ethereum-, Neo- oder Cardano-Blockchain können beispielsweise intelligente Verträge und Applikationen programmiert werden. Die Anzahl Kryptowährungen nimmt derzeit laufend zu – und der Markt wird letztlich entscheiden, welche davon bestehen werden.

Der Geldwettbewerb wird heute zwar durch die gesetzliche Privilegierung des Staatsgeldes verzerrt, indem beispielsweise ein Annahmezwang für die staatliche Währung gilt und man folglich noch nicht darum herumkommt, immer mal wieder zwischen dem staatlichen Geld und dem Geld seiner Wahl hin und her zu wechseln. Der Tausch zwischen Staatsgeld und Kryptogeld wird Nutzern jedoch durch immer raffiniertere und intuitivere Methoden vereinfacht. Bereits heute können Kunden mit speziellen EC-Karten an der Kasse bezahlen, welche Kryptoguthaben automatisch in staatliches Geld umwandeln. Umgekehrt bieten Anbieter wie etwa Coinbase Softwarelösungen für Unternehmen an, damit diese die von Kunden erhaltenen Kryptogelder (oder prozentual definierte Anteile davon) unmittelbar und automatisch in staatliches Geld umtauschen können.

Eine wesentliche Eigenschaft des Wettbewerbs ist jene, dass schlechte Angebote aufgrund der Wahlfreiheit von besseren verdrängt werden. Gleiches gilt für den Geldwettbewerb: Gutes Geld verdrängt tendenziell schlechtes Geld. Welches Geld

[23] Friedrich August von Hayek (1976). *Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies.* London: Institute of Economic Affairs.

nun gut oder schlecht ist, entscheiden letztlich die Nutzer aufgrund ihrer Präferenzen mit ihren Entscheidungen, die sie treffen. Es ist anzunehmen, dass die folgenden Faktoren eine wichtige Rolle bei dieser Entscheidungsfindung spielen dürften[24]:

- **Allgemeine Akzeptanz**: Wird ein Geld nicht breit akzeptiert, steigen die Transaktionskosten aufgrund erforderlichem Geldwechsel oder aufgrund der Suche nach Geschäftspartnern, welche das jeweilige Tauschmittel an Zahlung nehmen.
- **Seltenheit**: Das Geldangebot kann nicht beliebig vergrössert werden. Ansonsten verliert es seinen Wert.
- **Haltbarkeit**: Güter, die verderblich, empfindlich oder nur schwer gelagert werden können, eignen sich weniger als Geld.
- **Transferierbarkeit**: Es muss möglich sein, Geld ohne grosse Hürden und Kosten zu übertragen, damit es seine Tauschmittelfunktion erfüllen kann.
- **Wertstabilität**: Damit Geld freiwillig angenommen wird, sollte dieses im Wert nicht volatil sein oder ständig an Wert verlieren.
- **Teilbarkeit**: Damit Geld die Funktion des Tauschmittels erfüllen kann, muss es in möglichst kleinen Stückelungen zur Verfügung stehen.
- **Homogenität**: Geldeinheiten sollten untereinander austauschbar sein, da ansonsten individuelle Bewertungen nötig sind, die hohe Transaktionskosten verursachen.
- **Verifizierbarkeit**: Echte Geldeinheiten müssen von Fälschungen einfach unterscheidbar sein, um Transaktionskosten niedrig zu halten.

Der wesentliche Unterschied zwischen staatlichem Geld und Kryptowährungen mit Geldangebotsbegrenzungen liegt beim Faktor der «Seltenheit»: Staatliches Geld erfüllt zwar meistens dieses Kriterium. Die Produktion weiterer Einheiten ist jedoch mit derart tiefen Kosten verbunden und hängt von Entscheidungen von Beamten ab, auf die die wenigsten einen Einfluss haben. Folglich wird Vertrauen in die Disziplin von einer kleinen Gruppe von Menschen vorausgesetzt, dieses Geld knapp zu halten und somit die Werthaltigkeit zu schützen. Wie weiter oben bereits erläutert, ersetzen Kryptowährungen das Vertrauen in Menschen durch ein Vertrauen in ihre öffentlich einsehbaren Geldschöpfungs-Algorithmen. Durch die limitierte Geldmenge[25] versprechen viele Kryptowährungen im Gegensatz zur potenziell möglichen oder tatsächlich betriebenen expansiven Geldpolitik bei den Staatswährungen im Idealfall einen langfristigen Vorteil bezüglich der Geldwertstabilität und bei steigender Produktivität der Wirtschaft sogar einen zunehmenden Wert des Geldes bei konstanter Geldnachfrage. Hat der Bürger die freie Wahl, ob er sein Vermögen lieber in Geld halten möchte, das an Wert verliert, oder in Geld, das an Wert gewinnt, dürfte die Entscheidung klar ausfallen.

[24] Vgl. dazu: Aleksander Berentsen und Fabian Schär (2017). *Bitcoin, Blockchain und Kryptoassets – Eine umfassende Einführung*. Norderstedt: BoD. S. 16-17.

[25] Dies ist jedoch nicht bei allen Kryptowährungen der Fall. Einige Kryptowährungen haben kein absolut limitiertes Geldangebot. Ein Beispiel dafür ist Monero, bei welchem voraussichtlich ab dem Jahr 2022 für alle Zeiten pro geschürftem Block 0,6 – d.h. pro Jahr 157 788 – Moneroj geschöpft werden.

Die staatliche Geldpolitik könnte in ihren diskretionären Möglichkeiten aufgrund des sich intensivierenden Geldwettbewerbs zunehmend eingeschränkt werden. Hält sie weiterhin an ihrer ultraexpansiven Geldpolitik fest, dürften immer mehr Leute das Vertrauen in die künftige Werthaltigkeit des Staatsgeldes verlieren und dieses zugunsten besserer Alternativen abstossen, seien dies Kryptowährungen oder andere Geldformen. Durch diese Abwanderung von Nutzern hätte die Geldpolitik immer weniger Einfluss auf das wirtschaftliche Geschehen. Dies würde auch bedeuten, dass die Möglichkeit, die Zinsen politisch festzulegen, eingeschränkt würde und dem natürlichen, marktwirtschaftlichen Zins zunehmend grössere Bedeutung zukommen würde. Wenn der Zins vermehrt wieder die Zeitpräferenzen der Menschen abbildet anstelle politischer Willkür, schwindet die Gefahr der Fehlleitung knapper Ressourcen und von Wirtschaftskrisen, weil an die Investoren keine irreführenden Signale mehr ausgesendet werden, die in einem System manipulierter Zinsen an der Tagesordnung sind.

Die Herausforderungen und Schwächen von Kryptowährungen

Doch es gibt auch Gründe, die gegen eine breite Akzeptanz von Kryptowährungen sprechen. Die offensichtlichsten sind zum heutigen Zeitpunkt die technische Komplexität, welche – wie damals bei der Erfindung des Internets – zunächst durch nutzerfreundliche Anwendungen überwunden werden muss, die Betrugsanfälligkeit von Handelsplattformen für Kryptowährungen, sowie die hohe Fluktuation der Kurse, die dazu geführt hat, dass Kryptowährungen bislang eher als spekulatives Anlage-Investment, denn als Tauschmittel verwendet werden.

Aber auch die Hüter der staatlichen Geldpolitik finden verständlicherweise keinen Gefallen an der neuen Konkurrenz. Kryptowährungen schränken ihre Handlungsoptionen ein und schwächen ihre mächtige Position, in welcher sie Wirtschaft und Gesellschaft heute noch zu lenken vermögen. Wäre es da für die Regulatoren nicht naheliegend, Kryptowährungen einfach zu verbieten oder mindestens deren Benutzung regulatorisch stark zu begrenzen, um sich die Konkurrenz vom Leibe zu halten? Diese Möglichkeit besteht durchaus und wird von einigen Staaten bereits vollzogen.

Es bleibt jedoch anzumerken, dass ein Verbot nicht einer Beseitigung oder Zerstörung von Kryptowährungen gleichkommen würde – auch wenn es bestimmt eine Wirkung unter rechtschaffenen Bürgern haben dürfte, die sich nichts Illegales zuschulden kommen lassen möchten und folglich die Finger davon lassen. Denn aufgrund der Dezentralität der Kryptowährungen gibt es keinen zentralen Server, den die Regierungen ausfindig machen und abschalten könnten. Zwar könnte es gelingen, einzelne Netzwerk-Betreiber aus dem Verkehr zu ziehen. Angesichts der hohen Rechnerkapazitäten und Energiekosten, die manche «Proof-of-Work»-Kryptowährungen erfordern, ist etwa die Schliessung von «minining farms» nicht ausgeschlossen, die sich aus Kostengründen oft in Entwicklungsländern mit fragwürdigen rechtstaatlichen Prinzipien befinden. Jedoch erscheint es als ein Ding der Unmöglichkeit, das ganze

Netzwerk abzuschalten, wenn dieses erst einmal eine kritische Zahl von Knoten erreicht hat.

Es bestehen zudem Befürchtungen, dass Regierungen sogenannten «51-Prozent-Angriffe»[26] durchführen könnten, um die Kontrolle über ein Netzwerk zu erlangen. Diese sind aber erstens äusserst energie- und kostenintensiv und zweitens gibt es bereits unzählige Konkurrenten, auf welche die Kunden ausweichen könnten, sollte ein Angriff tatsächlich gelingen. Ein solcher «51-Prozent-Angriff» ist daher für eine Regierung von geringem Nutzen – auch wenn damit die betroffene Währung wohl einiges an Vertrauen einbüssen würde, sollte ein solcher gelingen.

Wahrscheinlich hätte ein Verbot von Kryptowährungen in Industrieländern, die schon seit längerer Zeit von wirklich katastrophalen Währungskrisen verschont geblieben sind, eine grössere Wirkung auf die Nutzung, wie in Ländern, welche in kürzerer Vergangenheit die schmerzvolle Erfahrung einer drastischen Währungsabwertung oder eines «Bail-in» machen mussten und in welchen das Vertrauen in die Währungshüter nachhaltiger gestört ist. Erfahrungen wie etwa jene in Argentinien – einem Land, das regelmässig von politisch induzierten Währungskrisen heimgesucht wird – zeigen, dass selbst strenge Kapitalverkehrskontrollen und das Verbot anderer Währungen wie etwa dem US-Dollar die Bürger nicht davon abhalten können, solche Gesetze zu umgehen und trotzdem alternative Währungen zu benützen. Ein Verbot hätte letztlich wohl die Wirkung, dass immer mehr wirtschaftliche Aktivitäten des betroffenen Landes auf Schwarzmärkte abwandern, wo voraussichtlich insbesondere mit jenen Kryptowährungen bezahlt werden dürfte, die besonders grossen Wert auf den Schutz der Privatsphäre und auf Anonymität legen.

Bei den Kryptowährungen, die nach dem «Proof-of-Work»-Prinzip funktionieren, besteht darüber hinaus die Gefahr, dass der Wettbewerb im «Mining» zu einem Monopol oder Oligopol führt, weil eine immer höhere Rechenleistung erforderlich wird, um überhaupt noch realistischerweise eine Chance zu haben, die gestellten Rechenaufgaben als erstes zu lösen und belohnt zu werden. Bei der Kryptowährung Bitcoin etwa befindet sich ein Grossteil der Mining-Aktivitäten mittlerweile unter der Kontrolle von sogenannten Mining-Pools, an denen sich Investoren beteiligen, die für sich alleine mit einem normalen Computer zuhause keine reelle Chance mehr hätten, die Belohnungen zu erhalten. Durch die Beteiligung von diversen Investoren an einem Mining-Pool kann der Pool jeweils Rechenleistung bündeln. Diese Entwicklung pervertiert allerdings die ursprüngliche Idee von Kryptowährungen als dezentral organisierte Alternative zu staatlichem Geld, und machen sie auch anfällig für staatliche In-

[26] Bei «51-Prozent-Angriffen» handelt es sich um Angriffe auf das Netzwerk, bei denen ein einzelner Netzwerkteilnehmer eine grosse Macht auf sich vereint, weil er dem Netzwerk eine prozentual grosse Rechenleistung zur Verfügung stellt und dadurch theoretisch einzelne Transaktionen blockieren oder Doppelausgaben tätigen könnte, indem er an einer alternativen Blockkette weiterarbeitet als der Rest des Netzwerks, die dann aufgrund seiner grossen Rechenleistung zur längsten Kette im Netzwerk werden würde.

terventionen. Zudem ist das System des Arbeitsnachweises äusserst energieintensiv.[27] Dies ist jedoch der Preis für eine hohe Sicherheit, weil «Denial-of-Service»-Angriffe nicht ohne entsprechenden Kostenaufwand initiiert werden können.

Als Alternative zum «Proof-of-Work» wurde das «Proof-of-Stake»-Modell erarbeitet, zu welchem etwa die Kryptowährungen Dash, Neo, Pivx und NavCoin gehören und zu welchem auch Ethereum übergeht. In einem solchen System validieren Besitzer der jeweiligen Kryptowährung jeweils nach dem Zufallsprinzip Blöcke und erhalten die neu ausgegebenen Münzen. Doch auch dieses Modell führte zu Kritik: Weil durch dieses Verfahren jene begünstigt werden, die bereits vermögend sind, besteht eine Tendenz zur einseitigen Bereicherung. Zudem werden Sicherheitsbedenken angemeldet, da ein «Proof-of-Stake»-System nicht die gleiche Sicherheit zu liefern vermag, wie ein «Proof-of-Work»-System, in welchem ein Akteur über 50% der Rechenleistung verfügen muss, um das System nachhaltig zu betrügen.

Ein weiterer Punkt, der Kryptowährungen an ihrer Verbreitung hindern könnte, ist ihre Skalierbarkeit. Die Blockgrösse der Kryptowährung Bitcoin etwa ist auf 1 Megabyte beschränkt. Je nach Umfang der einzelnen Transaktionen (die im Durchschnitt rund 226 Bytes gross sind) können in einem Block nur wenige tausend Transaktionen aufgenommen werden. Zwar wurde dieses Problem mit einer «Hard Fork» im August 2017, aus der Bitcoin Cash entstanden ist, adressiert, bei welchem die Blockgrösse auf 8 Megabytes erhöht wurde. Eine zu grosse Blockgrösse jedoch erfordert wiederum mehr Rechenleistung beim «Mining», was die Zentralisierung hin zu Mining-Pools weiter forcieren und somit die Dezentralität des Systems gefährden würde. Auf der anderen Seite können Kryptowährungen den Sprung zur Massennutzung nur dann schaffen, wenn sie die Skalierungsprobleme beheben können. Die Lösung wird sich wohl auf dem Dreieck Dezentralität, Skalierbarkeit und Sicherheit positionieren müssen, wobei das «Trilemma» darin besteht, dass ein System nur zwei dieser Eigenschaften erfüllen kann.[28] Die Community ist derzeit zerstritten in der Frage, in welche Richtung es weitergehen soll. Die Möglichkeit von sogenannten «Forks», also Gabelungen der Blockchain, macht es aber auch gar nicht nötig, dass hier ein Konsens bestehen muss. Der Wettbewerb zwischen den einzelnen Währungen wird zeigen, welche Projekte sich durchsetzen, weil sie am besten den Ansprüchen der Nutzer genügen.

Es gibt allerdings auch Ansätze ausserhalb des Blockchain-Ökosystems, die sich mit der Frage der Skalierung befassen. IOTA, die sich als Kryptowährung für das Internet der Dinge (IoT) bezeichnet, verspricht etwa skalierbare Transaktionen ohne Gebühren. IOTA basiert nicht auf einer Blockchain, sondern auf einer noch neueren «Tangle»-Technologie, einem zyklenlosen Graph aller Transaktionen im Netzwerk. Jeder Auslöser einer Transaktion muss zunächst zwei andere Transaktionen nach dem

[27] Vgl. dazu: Christopher Malmo (1. November 2017). *One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week*. Verfügbar unter: http://www.palada.net/index.php/2017/11/01/news-3997/
[28] Vgl. dazu: Christian Beckel (2017). *Skalieren Blockchains? Sorgen und Lösungsansätze*. Abrufbar unter: http://site.blocklab.de/2017/Skalierung/

Zufallsprinzip verifizieren, was es schwierig macht, «Double-Spend»-Angriffe auszuführen, wenn der Umfang des Netzwerks erst einmal eine gewisse Grösse erreicht hat. Wie sicher die Tangle-Technologe tatsächlich ist, muss allerdings erst noch getestet werden.

Wie bereits angesprochen, handelt es sich bei Kryptowährungen nicht wie oftmals behauptet, um Währungen, die ohne Vertrauen funktionieren. Zwar sind die Programmiercodes der meisten Kryptowährungen öffentlich einsehbar. Jedoch dürfte ausser den jeweiligen Experten kaum jemand wirklich verstehen, was sich hinter diesen komplexen Codes tatsächlich verbirgt. Im Grunde genommen ist also das Vertrauen in die Integrität und Expertise der Code-Schreiber Voraussetzung für Nicht-Experten zur Nutzung von Kryptowährungen. Es wäre naiv anzunehmen, dass Kryptowährungs-Programmierer a priori bessere Menschen wären als jene an den Schalthebeln der staatlichen Geldpolitik. Die Möglichkeit von Betrug und Machtmissbrauch darf nicht ignoriert werden. Daher wäre es wichtig, dass Kryptowährungen private Sicherungs- und Governance-Standards entwickeln und etablieren.

Kryptowährungen, insbesondere jene mit einer mengenmässigen Beschränkung, dürften die Gesellschaft auch vor kulturelle Herausforderungen stellen, die nicht zu unterschätzen sind: Insbesondere seit der Auflösung des Goldstandards 1971 herrscht praktisch in der ganzen Welt eine «Inflationskultur»[29], die unter anderem dadurch gekennzeichnet ist, dass der Wert des Sparens unterminiert wird und die Kosten der Verschuldung verhältnismässig sinken, dass kurzfristiges Denken an die Stelle von langfristigen Überlegungen rückt, und dass ansonsten schwierig finanzierbare Staatsaktivitäten durch wachsende Staatsschulden finanziert werden können und damit die Verstaatlichung der Gesellschaft und der Wirtschaft immer weiter voranschreiten. Staatliche Aktivitäten und immer dichter gewobene Auffangnetze haben folglich zunehmend die individuelle Eigenverantwortung erodieren lassen, sodass die Illusion entstand, dass «jedermann auf Kosten von jedermann leben» könne, wie das der Ökonom Frédéric Bastiat treffend formulierte.

Der aufkommende Wettbewerb der Währungen hätte zur Folge, dass solche Staatsaktivitäten künftig allenfalls nicht mehr in diesem Ausmass finanziert werden könnten, weil es sonst zu einem Exodus aus der dadurch abgewerteten Staatswährung kommen könnte. Es stellt sich die Frage, wie und ob eine Gesellschaft, die sich in vielen Bereichen an die staatliche Versorgung gewöhnt hat, mit diesem Umstand umgehen wird. Erfahrungen, die beim Zusammenbruch der DDR oder der Sowjetunion gemacht wurden, als die Bürger ebenfalls von der umfassenden Staatsversorgung in die Freiheit entlassen wurden, deuten hier auf einige Schwierigkeiten hin, welche kulturell bei derartigen Umstellungen gemeistert werden müssen. Nichtsdestotrotz wären solche Anpassungen im Sinne einer Ausweitung der Eigenverantwortung und der Selbstbestimmung jedes einzelnen aus liberaler Perspektive natürlich zu begrüssen.

[29] Vgl. dazu: Jörg Guido Hülsmann (2013). *Die Krise der Inflationskultur*. München: FBV.

Die weiteren Potenziale der Blockchain-Technologie

Nachdem nun die Schwächen und Herausforderungen von Kryptowährungen beleuchtet wurden, soll nachfolgend noch ein Blick auf das grosse Ganze geworfen werden. Denn die Blockchain-Technologie wird voraussichtlich nicht nur auf das Geldsystem und die Geldpolitik Auswirkungen haben. Im Grunde genommen ist sie geeignet, viele übliche Vermittlerfunktionen auszuschalten, die bislang das Vertrauen zwischen sich unbekannten Dritten hergestellt haben. Diese Veränderungen dürften signifikante Vorteile für die Lebensqualität aller bringen.

Geld kann dank der Blockchain-Technologie direkt von Person zu Person übermittelt werden, ohne dass dafür vertrauenswürdige Dritte wie Banken, Zentralbanken oder Clearingstellen vonnöten wären. Dadurch werden Überweisungen – insbesondere solche über Länder und Kontinente hinweg – wesentlich schneller und vor allem kostengünstiger, etwa mit Kryptowährungen wie IOTA, die ohne Transaktionsgebühren auskommen. Gerade im Zeitalter, in welchem persönliche finanzielle Daten der Menschen zwischen Staaten immer freizügiger ausgetauscht werden zwecks flächendeckender steuerlicher Unterdrückung, rücken auch Kryptowährungen wie Monero, Dash, Pivx, ZCash und NavCoin in den Fokus, zumal diese Währungen das Prinzip der finanziellen Privatsphäre der Nutzer hochhalten, indem beispielsweise Transaktionen nur noch sehr schwer nachverfolgt werden können. Natürlich können diese Währungen auch für illegale Geschäfte genutzt werden, sie dürfen aber nicht lediglich auf diesen Aspekt reduziert werden, auch wenn erwartet werden muss, dass die Staatencommunity ihre Gesetze in Sachen Geldwäscherei und Finanzierung von Kriminalität und Terrorismus auch dort anwenden wird.

Kryptowährungen ermöglichen auch jenen Bevölkerungsgruppen Zugang zur globalisierten Weltwirtschaft, die bislang vom heutigen Bankensystem ausgesperrt geblieben waren, weil sie die Kriterien der Banken nicht erfüllten, damit sie ein Bankkonto eröffnen konnten. In Nicaragua beispielsweise, dem Land mit dem zweitniedrigsten Bruttoinlandprodukt der Region Amerika, haben zwar nur 19 Prozent der Bevölkerung ein Bankkonto und nur 14 Prozent können einen Kredit aufnehmen, jedoch besitzen 93 Prozent ein Mobiltelefon[30], was ihnen den Zugang zu Kryptowährungen und Mikrokrediten in Kryptowährungen erlaubt. Insbesondere in Entwicklungsländern dürfte die Nutzung der Kryptowährungen deshalb zu einem signifikanten Wirtschaftswachstum führen.

Die Blockchain-Technologie ist nicht nur im Bereich der Geldüberweisungen nützlich: Besitzurkunden, Eigentumsnachweise, Geburts- und Sterbeurkunden, Bildungsnachweise, Heiratsurkunden, Patientenakten, aber auch Wahlen und Abstimmungen können fälschungssicher aufgezeichnet werden. Dies erleichtert die Aufbewahrung legitimer Rechte, die wiederum in schwierigen Regionen der Welt als Sicherheiten etwa gegen Darlehen vorgewiesen werden können. Als weitere Beispiele bietet ein Vermittler wie Ascribe Blockchain-basierte Lösungen für die Verwaltung und den

[30] Don Tapscott und Alex Tapscott (2016). *Die Blockchain Revolution*. Kulmbach: Börsenmedien AG. S. 223.

Verkauf digitaler Kunst. Weitere Anbieter bieten Plattformen für Produktgarantien, Fotos und Videos, das industrielle Internet der Dinge oder gar die DNA.

Technologieriesen wie Facebook, Twitter und Google, die ihre Umsätze zu einem grossen Teil durch die Nutzung von Kundendaten erzielen (Stichwort «Big Data»), sind ebenfalls von den Umwälzungen betroffen. In Kombination mit Verschlüsselungstechnologien ermöglicht die Blockchain-Technologie den Nutzern, wieder Herr über ihre persönlichen Daten zu werden. Der Anbieter Civic ist ein Beispiel für ein Projekt in diese Richtung. Es ist denkbar, dass man in Zukunft dafür bezahlt wird, wenn man Firmen seine persönlichen Daten zu Marketingzwecken zur Verfügung stellt oder wenn man sich Werbevideos von Produkten ansieht. Diese Einnahmen fliessen heute alleine an die Vermittler, die ihren Kunden zwar «kostenlose» Dienstleistungen wie Suchdienste, Video- oder Social Media-Plattformen zur Verfügung stellen, aber eben zum Preis der Überlassung wertvoller persönlicher Daten. Damit erstellen diese Firmen – in Kooperation mit staatlichen Organisationen – persönliche Profile der Bürger und ermöglichen den Aufbau eines Bespitzelungs- und Überwachungsstaates, der die schlimmsten Vorstellungen von George Orwell sogar noch übertrifft, wie etwa die Enthüllungen von Edward Snowden gezeigt haben.

Auch Zensur von unliebsamen Meinungen und Ansichten durch die «Gatekeeper» in klassischen oder sozialen Medien könnte bald der Vergangenheit angehören aufgrund der praktisch unmöglichen Manipulation der Blockchain und der dauerhaften Speicherung der Beiträge. Das Blockchain-basierte soziale Netzwerk Steemit geht beispielsweise in diese Richtung. Auch Prognosedienstleistungen könnten zumindest partiell von Blockchain-Prognosemärkten wie etwa Augur abgelöst werden.

Trendwende für die individuelle Freiheit?

Zusammenfassend darf konstatiert werden, dass die Blockchain-Technologie – sollten sich ihre Versprechen erfüllen – für die individuelle Freiheit ein Hoffnungsträger sein könnte, [1] weil sie manche staatliche Vermittler überflüssig macht, welche in der Vergangenheit oftmals ihre mächtige Position zu ihrem eigenen Vorteil missbraucht und welche mittels erzwungener Steuerfinanzierung oder gesetzlicher Privilegierung Ineffizienzen zementiert haben; [2] weil sie den Währungswettbewerb mindestens im Ansatz belebt und damit einerseits die staatliche Geldpolitik diszipliniert und andererseits Alternativen hervorbringen kann, welche in vielen Fällen besser in der Lage sind, das Privateigentum der Bürger zu schützen; [3] weil der Währungswettbewerb dem natürlichen Zins wieder zum Durchbruch verhelfen könnte, was wiederkehrende Finanz- und Wirtschaftskrisen unwahrscheinlicher machen würde; [4] weil die Blockchain-Technologie Millionen bisher von der Weltwirtschaft abgehängter Menschen in Entwicklungsländern Zugang zur globalisierten Wirtschaft ermöglicht und dadurch zu einem enormen Wohlstandswachstum in diesen Ländern beitragen könnte; und [5] weil sie den Bürgern in Kombination mit raffinierten Verschlüsselungsverfahren dabei helfen könnte, die Macht über ihre persönlichen Daten wiederzuerlangen und den allwissenden Überwachungsstaat in seine Schranken zu weisen.

Noch steckt die Blockchain-Technologie in den Kinderschuhen und hat enorme Herausforderungen zu bewältigen. Ebenso beeindruckend sind die Potenziale. Vorerst wird die Blockchain-Technologie für die mögliche Effizienzsteigerung bestehender Anbieter intensiv geprüft. Eine Alternative zu herkömmlichen Geldtransfers ist sie bereits in Nischenmärkten. Als eigentliche Währungen dienen Kryptowährungen derzeit ansatzweise vor allem in Entwicklungsländern mit katastrophaler Geldpolitik. Umstrittener unter freimarktwirtschaftlichen Ökonomen ist deren Wert als «immaterielle Güter», wie Kryptowährungen offiziell durch den regulatorischen Staat und Steuerbehörden sowie implizit durch Spekulanten und Investoren meist angesehen werden. Ob hier eine Blase platzen wird, ist genauso wahrscheinlich wie ungewiss.

Aus politökonomischer Sicht soll abschliessend festgestellt werden: Technologie ist kein Ersatz für Ideen. Ohne ein Verständnis und breite Unterstützung für die individuelle Freiheit, die freiwillige Zivilgesellschaft und die ungehinderte Marktwirtschaft ist es zweifelhaft, ob die Blockchain-Technologie zu mehr Freiräumen führen wird. Genauso gut können Technologien im Zeitalter einer vom Etatismus dominierten öffentlichen Meinung und politischen Kultur zur Durchsetzung gegenteiliger Ziele genutzt werden, etwa zur Beseitigung der finanziellen Privatsphäre infolge einer Abschaffung des Bargeldes und der Implementierung staatlicher Kryptowährungen, die wiederum zentral gesteuert werden und den Regierungen neue Methoden zur Überwachung und Kontrolle an die Hand geben. Nur der Einsatz für ein liberales Meinungsklima sowie für den Schutz der Würde des Individuums, seiner Privatsphäre und seines Eigentums, kann allenfalls verhindern, dass freimarktwirtschaftliche Alternativen durchreguliert oder verboten und durch staatlich kontrollierte und privilegierte Angebote verdrängt werden.

Die Erfindung des Internets wurde vor allem deshalb rasch von einer breiten Öffentlichkeit adaptiert, weil Regulatoren gegenüber dieser neuen Technologie zurückhaltend auftraten und Entwickler daher rasch massenmarkttaugliche Anwendungen wie etwa nutzerfreundliche Internet-Browser entwickeln konnten, ohne vom Staat daran gehindert zu werden. In der Schweiz haben sich die Regulatoren in Bezug auf Kryptowährungen bislang glücklicherweise zurückgehalten, was eine wichtige Voraussetzung dafür ist, dass sich neue Blockchain-Firmen im «Crypto Valley» in den Kantonen Zug und Zürich ansiedeln und damit einen Innovationshub bilden können, aufgrund welchem der Fortschritt schnell vonstattengehen könnte. Priorität hat folglich die Aufklärung für eine liberale Ordnungspolitik, welche Innovation nicht behindert und den nötigen Freiraum für unternehmerische Experimente und Risiken lässt. Jenseits des Schutzes des Privateigentums und des Kampfs gegen Betrug ist auch im Gebiet der Blockchain-Technologie auf innovationshemmende und -hinderliche Regulierungen zu verzichten.

Nicht anders verhält es sich angesichts einer möglichen Strukturerhaltungspolitik. Wenn Veränderungen anstehen, versuchen die potenziellen Verlierer oftmals, die Politik durch intensives Lobbying dazu zu bewegen, Unternehmen und Arbeitsplätze zu schützen, die unrentabel geworden sind. Eine solche Strukturerhaltungspolitik behindert nicht nur Innovation und Fortschritt, sondern fördert auch die Verschwendung

knapper Ressourcen. Genauso wie es sinnlos gewesen wäre, beim Aufkommen von persönlichen Computern Arbeitsplätze in der Schreibmaschinen-Industrie zu retten, wäre es widersinnig, allfällige überflüssige Funktionen retten zu wollen, damit Leute auf Kosten anderer Arbeiten verrichten, die niemandem mehr einen Nutzen stiften. Im Sinne eines effizienten Ressourceneinsatzes und der Förderung von wohlstandsschaffenden Innovationen ist daher auf eine Strukturerhaltungspolitik zu verzichten.

LIBERALES INSTITUT

Impressum

Liberales Institut
Rennweg 42
8001 Zürich, Schweiz
Tel.: +41 (0)44 364 16 66
Fax: +41 (0)44 364 16 69
libinst@libinst.ch

Alle Publikationen des Liberalen Instituts finden Sie auf www.libinst.ch.

Disclaimer