V. Kryptowährungen: ein Blick hinter den Hype

Vor nicht einmal zehn Jahren erfunden und zunächst als Kuriosität betrachtet, stehen Kryptowährungen[1] heute im Fokus des Interesses von Firmen, Konsumenten und Zentralbanken. Besondere Aufmerksamkeit erweckt ihr Anspruch, Vertrauen in etablierte Institutionen wie Geschäfts- und Zentralbanken durch Vertrauen in neue, komplett dezentralisierte Systeme auf Basis des Blockchain-Konzepts und der damit verbundenen Distributed-Ledger-Technologie zu ersetzen.

Dieses Kapitel beschäftigt sich mit der Frage, ob Kryptowährungen langfristig eine Rolle im Geldsystem spielen können. Oder anders ausgedrückt: Gibt es überhaupt Probleme, für die Kryptowährungen in ihrer heutigen Form eine Lösung bieten? Das Kapitel beginnt mit einem geschichtlichen Überblick. Zahlreiche Episoden geldpolitischer Instabilität und Währungen, die bald wieder Geschichte waren, zeigen, dass die institutionelle Absicherung des Geldes eine zentrale Rolle spielt. Damit das Geldsystem funktioniert, muss man sich stets darauf verlassen können, dass das Geld seinen Wert behält. Und damit das Geld seinen ureigensten Zweck als Koordinationsinstrument erfüllt, muss die Geldmenge mit der Wirtschaft mitwachsen und elastisch auf Nachfrageschwankungen reagieren. Diese Überlegungen sprechen für ein solides institutionelles Fundament, was wiederum erklärt, wieso wir unabhängige und zur Rechenschaft verpflichtete Zentralbanken haben.

Nach dem geschichtlichen Überblick folgt eine thematische Einführung zu Kryptowährungen. Dabei werden auch die ökonomischen Grenzen der dezentralisierten Vertrauensbildung erörtert. So wie das Vertrauen generiert wird, lässt es sich nur aufrechterhalten, wenn die Rechenleistung weitgehend unter der Kontrolle ehrlicher Netzwerkteilnehmer ist, die gesamte Transaktionshistorie von allen Anwendern validiert wird und die Kryptogeldmenge durch das Protokoll festgelegt ist. Die dezentrale Konsensbasis für die Transaktionserfassung ist jedoch fragil. Damit ist nicht nur die Finalität einzelner Transaktionen infrage gestellt; auch der technische Ausfall einer Kryptowährung – und somit ein Totalverlust – ist nicht auszuschließen. Aber auch wenn eine Kryptowährung wie vorgesehen funktioniert: Technisch ist das System ineffizient, und der Energieverbrauch ist enorm. Kryptowährungen können nicht mit der Transaktionsnachfrage mitwachsen, sind anfällig für Systemüberlastungen und unterliegen starken Kursschwankungen. Insgesamt ist die dezentralisierte Technologie, auf der Kryptowährungen basieren, bei aller technischen Raffinesse keine zweckmäßige Alternative zum institutionell abgesicherten Geld.

Die Technologie an sich könnte allerdings vielsprechend für andere Anwendungen sein, etwa für die vereinfachte Abwicklung von Finanztransaktionen. Doch auch das muss sich erst noch zeigen. Angesichts der vielen Fragen, die Kryptowährungen aufwerfen, wird abschließend erörtert, wie die Politik darauf reagieren sollte – sowohl bezüglich Regulierung der privatwirtschaftlichen Anwendung der Technologie und Verhinderung der missbräuchlichen Verwendung von Kryptowährungen, als auch im Hinblick auf die heiklen Fragen, die sich durch die Ausgabe von Digitalgeld durch Zentralbanken ergeben.

Der Vormarsch der Kryptowährungen in einem größeren Kontext betrachtet

Zunächst stellt sich die Frage, ob die neue Technologie das bestehende Geldsystem wirklich sinnvoll ergänzen kann. Um dies zu beurteilen, sollte man den Fokus zu erweitern und sich zunächst mit der fundamentalen Funktion des Geldes in der Wirtschaft und mit den Lehren aus gescheiterten privaten Geldexperimenten auseinandersetzen.[2]

Eine kurze Geschichte des Geldes

Geld spielt durch seine Funktion als Tauschmittel eine zentrale Rolle in der Wirtschaft. Vor seiner Entstehung vor Tausenden von Jahren wurden Güter hauptsächlich mit der Aussicht auf eine spätere Gegenleistung (d.h. auf Schuldscheinbasis) gehandelt.[3] Doch mit wachsender Bevölkerung und im Zuge der ökonomischen Entwicklung wurde das Schuldscheinsystem immer komplexer und ließ sich schwieriger aufrechterhalten. Dazu kam noch das Ausfall- und Abwicklungsrisiko. Die Antwort auf die Komplexität und die diesbezüglichen Vertrauensprobleme war die Schaffung von Geld und geldausgebenden Institutionen.

Geld erfüllt drei fundamentale, ineinandergreifende Funktionen: Erstens lassen sich mithilfe von Geld Verkaufspreise vergleichen und Werte darstellen (Recheneinheit). Zweitens geht jemand, der gegen Geld etwas verkauft, davon aus, dass er seinerseits das Geld für Käufe nutzen kann (Tauschmittel). Drittens lässt sich mit Geld die Kaufkraft für später bewahren (Wertaufbewahrungsmittel).[4]

Damit Geld diese Funktionen erfüllen kann, muss es überall gleich viel wert sein, und dieser Wert muss stabil bleiben: Eine Verkaufsentscheidung lässt sich einfacher treffen, wenn man sich darauf verlassen kann, dass der Verkaufserlös eine garantierte Kaufkraft hat und diese behält. Diesen Anspruch erfüllt aufgrund seines intrinsischen Wertes auch reines Warengeld, wie etwa Salz oder Getreide. Warengeld an sich fördert den Handel aber nicht effektiv: Es ist vielleicht nicht immer verfügbar, teuer in der Herstellung und unpraktisch als Tauschmittel, und gegebenenfalls begrenzt haltbar.[5]

Im Laufe der ökonomischen Entwicklung wurde es immer wichtiger, ein praktischeres Zahlungsmittel zur Verfügung zu haben, das mit der Nachfrage mitwächst, Handelsansprüchen gerecht wird und werthaltig ist. Die größte Herausforderung allerdings bestand stets darin, das Vertrauen in das institutionelle Fundament des Geldsystems aufrechtzuerhalten. Als Lösung dafür kristallisierte sich die Ausgabe des Geldes durch zentrale öffentliche Stellen heraus, und zwar rund um die Welt, unter verschiedenen Rahmenbedingungen und zu unterschiedlichen Zeitpunkten. Schon in der Antike wurde der Münzwert durch das jeweilige Herrscherbild garantiert. Später konnten Händler die Kosten und das Risiko, mit großem Münzgepäck zu reisen, mithilfe von Bankwechseln minimieren.[6]

Die Geschichte hat aber auch das Spannungsfeld zwischen flexibler Geldversorgung und schneller Geldentwertung aufgezeigt.[7] Rückblickend waren längere Perioden mit stabilem Geld viel eher die Ausnahme als die Regel. Die Geschichte des Geldes ist ein regelrechter Währungsfriedhof, den man in diversen Museen weltweit besichtigen kann, beispielsweise im British Museum in London im Ausstellungsraum Nr. 68. Steine, Muscheln, Tabak, unzählige Münzen, Scheine und viele andere Objekte haben ihre Rolle als Tauschmittel verloren und ihren Weg dorthin gefunden. Einige

dieser Zahlungsmittel fielen dem Ausbau des Handels und der Wirtschaftstätigkeit zum Opfer, weil ihre Verwendung im größeren Rahmen unpraktisch war. Andere verloren mit der Schwächung oder dem Sturz des dahinter stehenden politischen Systems ihre Bedeutung. Viele andere wiederum verschwanden in der Versenkung, weil das Vertrauen in ihre Werthaltigkeit nicht mehr gegeben war.

Wie die Geschichte zeigt, kann das Geldwesen fragil sein, unabhängig davon, ob Geld von privat getragenen Stellen ausgegeben wird, also unter Konkurrenzbedingungen, oder durch eine staatliche Stelle, die über ein Geldausgabemonopol verfügt. Das Geld, das von einer Bank ausgegeben wird, ist nur so viel wert wie der jeweilige Deckungsstock. Zu den Aufgaben der Banken zählt die Risikotransformation, woraus folgt, dass im Extremfall das Vertrauen in privat ausgegebenes Geld über Nacht schwinden kann. Aber auch staatlich gedeckte Geldsysteme, bei denen der Staat die Aufgabe übernimmt, das Vertrauen ins Geld zentral zu sichern, haben nicht immer gut funktioniert. Es gab sogar krasse Fälle von Missbrauch: So ging etwa die betrügerische Münzentwertung in deutschen Kleinstaaten im frühen 17. Jahrhundert als Kipper- und Wipperzeit in die Geschichte ein.[8] Aber es gibt unzählige andere Beispiele, auch aus der Gegenwart, etwa in Venezuela oder Zimbabwe. Die Vermeidung von staatlichem Missbrauch war daher nicht zuletzt eine der treibenden Kräfte bei der institutionellen Ausgestaltung des Geldsystems.

Die Suche nach einer soliden institutionellen Absicherung des Vertrauens ins Geld führte letztlich zum Aufbau der heutigen Zentralbanken. Ein erster Schritt in diese Richtung war die Gründung öffentlicher Banken in einer Reihe europäischer Stadtstaaten im Zeitraum 1400–1600. Sie sollten den Handel durch die Ausgabe hochwertiger und effizienter Zahlungsmittel erleichtern und durch die Übernahme diverser Abrechnungs- und Abwicklungsschritte zentralisieren. Mit Sitz in Handelszentren wie Amsterdam, Barcelona, Genua, Hamburg und Venedig brachten diese Banken den internationalen Handel und die Wirtschaft insgesamt zum Florieren.[9] Viele dieser Banken spielten nach und nach eine ähnliche Rolle wie die heutigen Zentralbanken. Des Weiteren wurden Zentralbanken, wie wir sie heute kennen, oft auch direkt als Reaktion auf schlechte Erfahrungen mit einem dezentralen Geldwesen gegründet. So führten in den USA letztlich Insolvenzen nicht zentral regulierter Banken zur Gründung des Federal Reserve System.

Geldwesen und Zahlungsverkehr heute

Die unabhängige Zentralbank ist heute *der* Garant dafür, dass wir Vertrauen in unser Geld haben können. Sie steht zum einen für klare geldpolitische und finanzstabilitätspolitische Zielvorgaben und zum anderen für operative, instrumentelle und administrative Unabhängigkeit sowie darüber hinaus für demokratische Rechenschaftspflicht, um politische Unterstützung und Legitimität auf breiter Basis sicherzustellen. Eine stabile Währung ist im allgemeinen wirtschaftspolitischen Interesse, und dieses Ziel lässt sich mit einer unabhängigen Zentralbank weitgehend erreichen.[10] Unter diesen Rahmenbedingungen kann Geld folgerichtig definiert werden als „unverzichtbare gesellschaftspolitische Konvention, hinter der eine rechenschaftspflichtige Institution der öffentlichen Hand steht, die das Vertrauen der Bevölkerung genießt".[11]

In nahezu allen modernen Volkswirtschaften übernimmt die Zentralbank die Geldversorgung gemeinsam mit dem privaten Bankensektor, wobei die Zentralbank der Systemmittelpunkt ist. Der Massenzahlungsverkehr wird in erster Linie über

elektronische Bankeinlagen abgewickelt, während die Zahlungen zwischen den Banken auf Basis von deren Zentralbankguthaben erfolgen. In diesem Zweistufensystem der Geldschöpfung wird das Vertrauen ins Geldwesen durch unabhängige und rechenschaftspflichtige Zentralbanken generiert, wobei die Zentralbankguthaben durch die Anlagen der Zentralbank und ihre operativen Regeln abgesichert sind. Vertrauen in die Bankeinlagen wiederum wird durch eine Vielzahl von Mitteln geschaffen, darunter die Bankenregulierung und -aufsicht sowie Einlagensicherungssysteme, wobei dahinter letztlich vielfach der Staat steht.

Im Rahmen der Erfüllung ihres Mandats zur Sicherstellung stabiler Zahlungsmittel spielen die Zentralbanken eine aktive Rolle bei der Banken- und Zahlungssystemaufsicht und treten teilweise auch als nationaler Zahlungssystembetreiber auf. So ist es Aufgabe der Zentralbank, dafür zu sorgen, dass der Zahlungsverkehr reibungslos funktioniert und die Versorgung mit Zentralbankgeld sichergestellt ist und angemessen auf Nachfrageschwankungen reagiert, auch auf Intraday-Basis. Mit anderen Worten: Die Zentralbank trägt die Verantwortung für eine elastische Geldversorgung.[12]

Dank der aktiven Mitwirkung der Zentralbank sind die diversen Zahlungsverkehrssysteme heute sicher, kosteneffizient und skalierbar, und man kann sich darauf verlassen, dass eine in Auftrag gegebene Zahlung auch wirksam, d.h. final, ist.

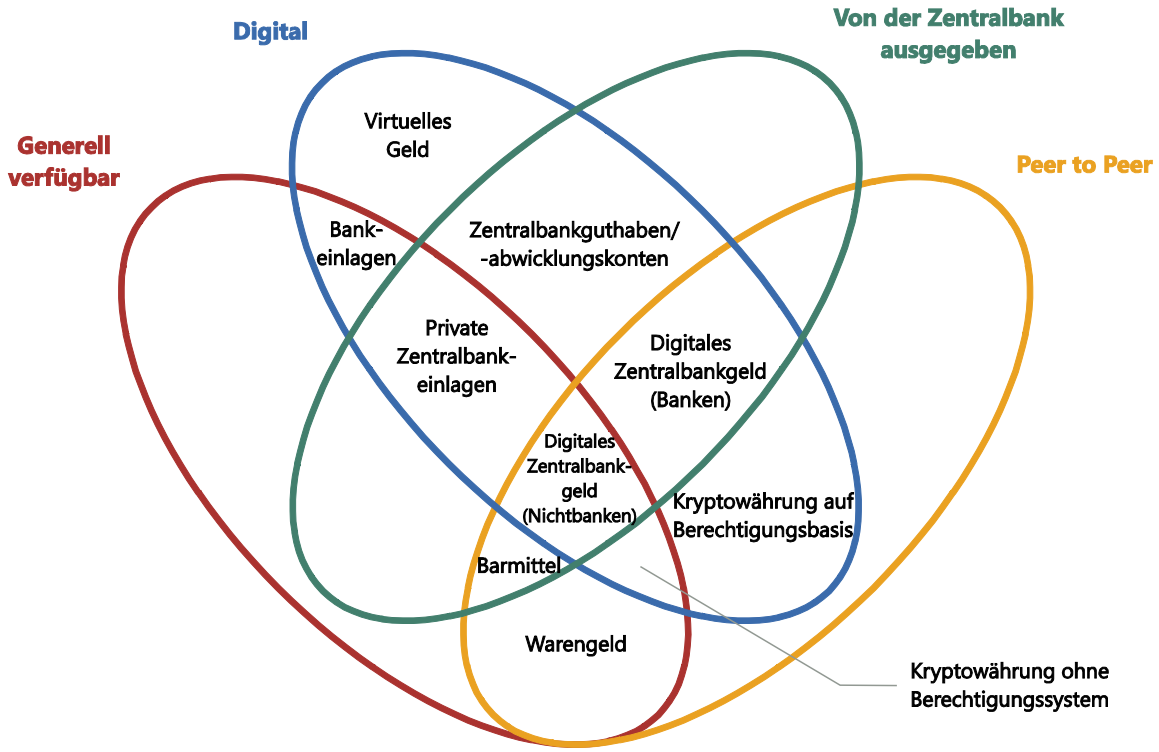
Hohe und stark steigende Volumina können weitgehend ohne missbräuchliche Vorfälle und kostengünstig verarbeitet werden. Für die Sicherheit und Kosteneffizienz spielt der Faktor Skalierbarbeit eine große Rolle. In den heutigen hochentwickelten Volkswirtschaften entspricht der Zahlungsverkehr dem Vielfachen des BIP. Trotz des hohen Volumens schlägt sich eine Ausweitung des Zahlungsverkehrs nicht proportional in den Kosten nieder. Das ist wichtig, denn der Erfolg eines jeden Geld- und Zahlungsverkehrssystems steht und fällt mit der Größe des Nutzerkreises: Je größer der Teilnehmerkreis, desto höher der Anreiz zur Nutzung des Systems.

Man muss sich aber nicht nur darauf verlassen können, dass das Geld sicher ist; man muss sich auch darauf verlassen können, dass Zahlungen prompt und reibungslos erfolgen. Operativ ist daher möglichst dafür zu sorgen, dass beauftragte Zahlungen auch tatsächlich durchgeführt werden (final sind) und – damit zusammenhängend – dass es möglich ist, eventuell nicht korrekt ausgeführte Transaktionen zu beanstanden. Finalität verlangt, dass das System weitgehend betrugssicher und operativ robust ist, sowohl auf der Ebene einzelner Transaktionen als auch insgesamt. Eine starke Aufsicht und die Rechenschaftspflicht der Zentralbank sind eine wichtige Voraussetzung für finale Zahlungen und damit ein wesentlicher Vertrauensfaktor.

Während der Zahlungsverkehr heute letztlich weitgehend zentralbankgestützt erfolgt, ist im Lauf der Zeit eine breite Palette an öffentlichen und privaten Zahlungsmitteln entstanden. Die verschiedenen Formen des Geldes können am besten anhand einer stilisierten Blume veranschaulicht werden (Grafik V.1).[13]

Anhand der stilisierten Geldblume lassen sich vier wesentliche Merkmale unterscheiden: von wem und in welcher Form Geld ausgegeben wird, wer Zugriff auf Geld hat, und auf welchem Weg der Transfer von Geld erfolgt. Ausgegeben werden kann das Geld von einer Zentralbank, einer Bank oder – wie beim Warengeld – von niemandem. Es kann sich dabei um physisches Geld handeln (etwa um Metallmünzen oder Banknoten) oder um Digitalgeld. Geld kann weitreichend verfügbar sein (wie Geschäftsbankeinlagen) oder eingeschränkt verfügbar (wie Zentralbankguthaben). Der Geldtransfer schließlich kann entweder direkt zwischen den Beteiligten (Peer to Peer) oder wie bei Einlagen über einen zentralen Intermediär erfolgen. Geld existiert

Klassifizierung von Geld anhand einer stilisierten Geldblume Grafik V.1



Quelle: Nach M. Bech und R. Garratt, „Kryptowährungen von Zentralbanken", *BIZ-Quartalsbericht*, September 2017.

in der Regel entweder wertbasiert (auf Token-Basis) oder kontenbasiert (auf Account-Basis). Bei wertbasierten Systemen kommen Werte wie Banknoten oder Münzen zum Einsatz. Sie eignen sich für den direkten Geldtransfer; wichtig ist dabei allerdings, dass der Zahlungsempfänger in der Lage ist, die Zahlungsmittelechtheit festzustellen – wobei beim Bargeld etwaige Geldfälschungen das Problem sind. Kontenbasierte Systeme wiederum hängen grundlegend von der Möglichkeit ab, die Identität der Kontoinhaber feststellen zu können.

Kryptowährungen: das trügerische Versprechen der dezentralen Vertrauensbildung

Halten Kryptowährungen, was sie versprechen? Oder sind sie ein Kandidat für das Kuriositätenkabinett? Um diese Fragen beantworten zu können, bedarf es zunächst präziserer Definitionen. Ferner ist es wichtig, die Technologie zu verstehen und die damit zusammenhängenden ökonomischen Grenzen zu erörtern.

Geldblume mit neuem Blütenblatt?

Kryptowährungen beanspruchen für sich, das Geldsystem zu revolutionieren, und versprechen, mit technischen Mitteln für das Vertrauen in ihre Werthaltigkeit zu sorgen. Kryptowährungen basieren auf drei Elementen: Erstens gibt es ein Regelwerk (Protokoll genannt); wie die Teilnehmer Transaktionen abwickeln können, ist per

Computercode festgelegt. Zweitens wird die gesamte Transaktionshistorie buchmäßig (in einem sog. Ledger) erfasst. Drittens erfolgt das Aktualisieren, Speichern und Lesen der Transaktionsdaten nach den Regeln des Protokolls. Mit diesen drei Elementen, so die Argumentation der Befürworter, ist eine Kryptowährung immun gegen etwaige fehlgeleitete Anreize im Bankensystem oder staatlicherseits.

Geht man von der Klassifizierung des Geldes in Form ein stilisierten Blume aus, so vereinen Kryptowährungen drei wesentliche Geldmerkmale auf sich. Erstens handelt es sich um Digitalgeld, das praktisch in der Handhabung sein soll und Fälschungen und betrügerische Transaktionen mit Verschlüsselung verhindert. Zweitens handelt es sich um privat geschöpftes Geld, für das aber niemand bürgt (d.h., es gibt kein Einlösungsversprechen) und dessen Wert sich nur von der Erwartungshaltung ableitet, dass es von anderen akzeptiert wird. Damit ähneln Kryptowährungen dem Warengeld (ohne jedoch einen intrinsischen Nutzwert zu haben). Drittens schließlich lassen sie sich direkt (Peer to Peer) digital übertragen.

Was Kryptowährungen von anderem privatem Digitalgeld wie Bankeinlagen unterscheidet, ist die Tatsache, dass der digitale Geldtransfer direkt zwischen den Beteiligten erfolgt. Digitale Bankkonten gibt es schon seit Jahrzehnten. Und privat ausgegebene „virtuelle Währungen", wie sie z.B. im Internet bei Massen-Gemeinschaftsspielen wie World of Warcraft verwendet werden, gab es schon zehn Jahre vor den Kryptowährungen. Typisch für Kryptowährungen ist allerdings, dass der Geldtransfer grundsätzlich dezentral, ohne Zwischenschaltung einer zentralen Gegenpartei, erfolgen kann.

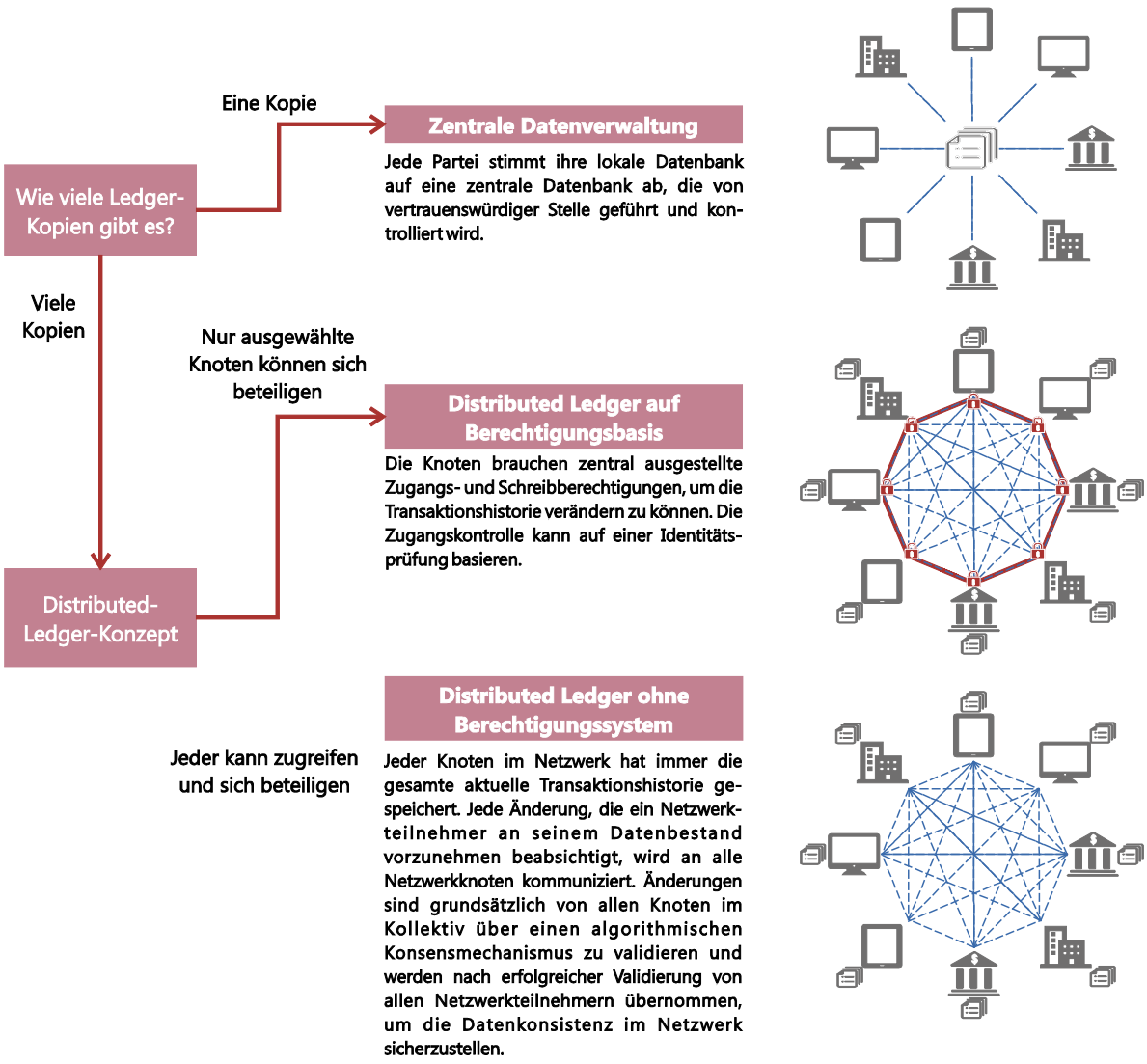
Die Distributed-Ledger-Technologie bei Kryptowährungen

Die technologische Herausforderung beim direkten digitalen Transfer liegt darin, zu verhindern, dass ein bestimmter Betrag mehr als einmal ausgegeben wird (Double-Spending-Problem). In digitaler Form lässt sich Geld leicht duplizieren und kann somit in betrügerischer Absicht mehrmals ausgegeben werden. Digitale Daten lassen sich leichter reproduzieren als physische Banknoten. Um das Problem der Duplizierbarkeit beim Digitalgeld in den Griff zu bekommen, müssen alle Transaktionen irgendwo erfasst werden. Vor den Kryptowährungen war dies nur durch Erfassung und Validierung an zentraler Stelle möglich.

Kryptowährungen lösen das Problem etwaiger Mehrfachausgaben dadurch, dass die Daten von allen Nutzern gemeinsam in Form eines „verteilten Kontenbuchs" (Distributed Ledger) verwaltet werden. Dabei wird die gesamte Transaktionshistorie quasi in einer Datei (man denke an ein Arbeitsblatt in Microsoft Excel) beginnend mit der Erstausgabe von Kryptowährungen fortlaufend erfasst, wobei die Historie stets bei jedem einzelnen Nutzer auf den neuesten Stand gebracht wird. So kann jeder Anwender direkt anhand seiner lokalen Kopie der Transaktionshistorie feststellen, ob eine rechtmäßige Zahlung (d.h. ohne Double-Spending-Versuch) erfolgte.[14]

Vergleich der Konzepte zur Verwaltung der Transaktionshistorie

Grafik V.2



		Privates elektronisches Geld auf Papiergeldbasis	Privat ausgegebene Kryptowährungen	
			Auf Berechtigungsbasis	Ohne Berechtigungssystem
1	Datenverwaltung	Zentrale Kontenführung bei einer Bank/einem sonstigen Finanzinstitut	Distributed-Ledger-Konzept	
2	Validierung (Vermeidung von Mehrfachzahlungen)	Konzept der Kundenidentifizierung	Peer-to-Peer-Konzept: Ob Werte bereits ausgegeben wurden, ist dezentral anhand der Transaktionshistorie überprüfbar	
3	Transaktionsverarbeitung	Kontoführung durch die Bank	Aktualisierung der Transaktionshistorie durch ausgewählte Trusted Nodes	Aktualisierung der Transaktionshistorie durch Proof of Work (Regel: es gilt die jeweils längste Kette)
4	Finalität/Abwicklung	Finale Abwicklung erfolgt zentralbankseitig	Abwicklung erfolgt in Kryptowährung	Finalität ist eine Wahrscheinlichkeitsfrage (aufgrund der Regel, dass jeweils die längste Kette gilt)
5	Elastizität der Geldmenge	Innertageskredit etc. im Ermessen der Zentralbank	Protokolländerungen durch Trusted Nodes	Im Protokoll festgelegt
6	Vertrauensbildende Mechanismen	(Zentral-)Bankenreputation, Bankenaufsicht, Kreditgeber der letzten Instanz, Tenderbestimmungen, Zentralbankunabhängigkeit/-rechenschaftspflicht, Geldwäsche- und Terrorismusfinanzierungsregeln, Cybersicherheit	Reputation der ausgebenden Firmen/Knoten Trusted Nodes (unterliegen eventuell teilweise der Aufsicht)	Proof of Work bedingt überwiegend ehrlich erbrachte Rechenleistungen

Quellen: Nach H. Natarajan, S. Krause und H. Gradstein, „Distributed ledger technology (DLT) and blockchain", Weltbankgruppe, *FinTech Note*, Nr. 1, 2017; BIZ.

Während die Nutzung der Distributed-Ledger-Technologie allen Kryptowährungen gemein ist, lassen sich je nach Fortschreibung der Transaktionshistorie generell zwei Architekturformen unterscheiden, die entweder auf Berechtigungsbasis (permissioned) oder ohne Berechtigungssystem (permissionless) funktionieren (Grafik V.2).

Kryptowährungen auf Berechtigungsbasis sind herkömmlichen Zahlungsverkehrsmechanismen insofern ähnlich, als die Transaktionshistorie nur an Systemknoten von vertrauenswürdigen und daher mit speziellen Berechtigungen ausgestatteten Teilnehmern (Trusted Nodes) aktualisiert werden kann. Diese Systemknoten werden von einer zentralen Stelle, z.B. vom Entwickler der Kryptowährung, bestimmt und auch von ihr überwacht. Obwohl also anders als im herkömmlichen Geldsystem die Transaktionsdaten dezentral (statt zentral) gespeichert werden, besteht insofern eine Gemeinsamkeit, als letztlich bestimmte Institutionen vertrauensbildend wirken.[15]

Viel radikaler in ihrer Abwendung von dem herkömmlichen institutionsbasierten System setzt eine zweite Kategorie von Kryptowährungen auf eine komplett dezentrale Lösung ohne Berechtigungssystem (permissionless) zur Vertrauensbildung. Die Transaktionshistorie kann nur bei Konsens unter den Währungsteilnehmern fortgeschrieben werden, wobei die Teilnahme jedem offen steht und niemand über spezielle Schreibberechtigungen verfügt.

Das Konzept der Kryptowährungen ohne Berechtigungssystem wurde am Beispiel Bitcoin[16] in einem Weißbuch von einem anonymen Programmierer(team) unter dem Pseudonym Satoshi Nakamoto dargelegt, wobei als spezielle Form der Distributed-Ledger-Technologie das Blockchain-Konzept eingeführt wurde. Bei der Blockchain wird die dezentral verwaltete Transaktionshistorie blockweise aktualisiert, wobei durch die Aneinanderreihung der Transaktionsblöcke unter Einsatz von Verschlüsselungsverfahren eine Kettenstruktur entsteht. Dieses Prinzip wurde inzwischen bei zahllosen anderen Kryptowährungen angewandt.[17]

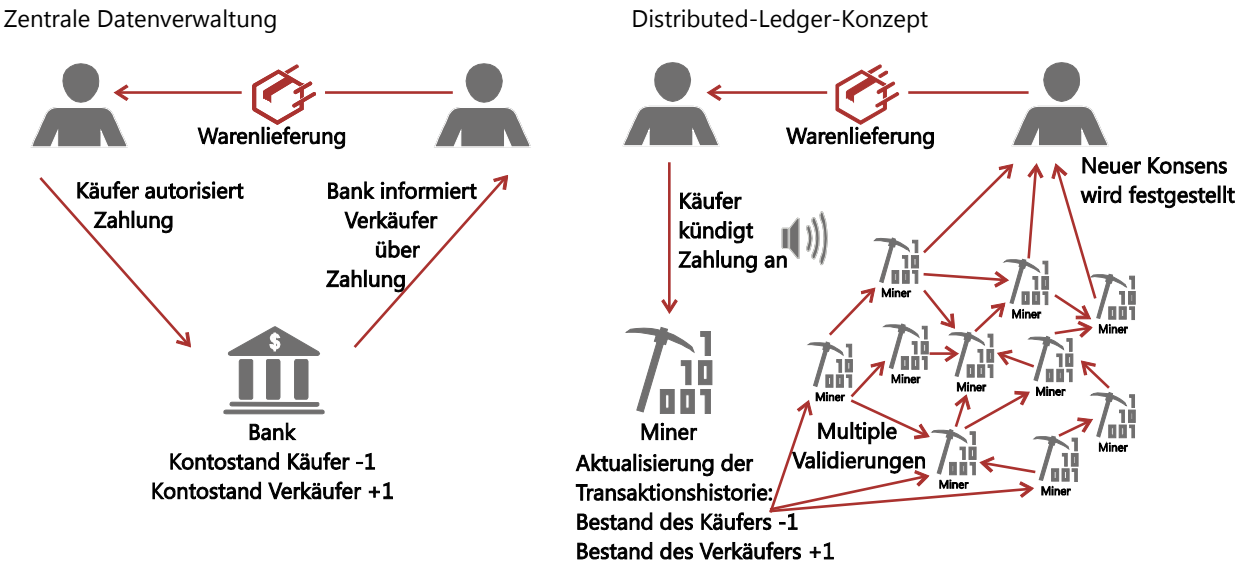
Bei den ohne Berechtigungssystem funktionierenden Kryptowährungen auf Blockchain-Basis unterscheidet man zwischen Teilnehmern, die eine spezielle Kontoverwaltungsfunktion haben (Miner), und den übrigen Nutzern mit einem reinen Transaktionsinteresse. Diese Kryptowährungen basieren im Grunde auf einer simplen Idee: Die Transaktionshistorie wird nicht zentral bei einer Bank erfasst (Grafik V.3 links), sondern von einem Miner aktualisiert und danach von allen Nutzern und Minern auf ihren jeweiligen Rechnern neu abgespeichert (Grafik V.3 rechts).[18]

Das Herzstück des Kryptowährungssystems ist die Umsetzung eines Regelwerks (Protokoll), das das Anreizsystem für alle Teilnehmer derart austariert, dass das Zahlungssystem technisch auch ohne vertrauenswürdige zentrale Instanz verlässlich funktioniert. Zum einen regelt das Protokoll die Geldmenge, um einer Geldentwertung entgegenzuwirken – im Fall von Bitcoin etwa ist der Umlauf bei 21 Mio. Bitcoins gedeckelt. Zum anderen ist das Protokoll darauf ausgelegt, dass alle Teilnehmer die Regeln aus purem Eigeninteresse befolgen und sich somit ein selbsttragendes Gleichgewicht einstellt. In diesem Zusammenhang sind drei wesentliche Aspekte zu nennen.

Erstens bestimmen die Regeln, dass die Fortschreibung der Transaktionshistorie mit einem bestimmten Aufwand verbunden ist, der sich meistens daraus ergibt, dass die Aktualisierungen nur mit einem entsprechenden Leistungsnachweis (Proof of Work) möglich sind. Konkret ist die Erbringung einer bestimmten Rechenleistung mathematisch nachzuweisen, was wiederum eine entsprechend teure Ausstattung erfordert und stromintensiv ist. Dabei ist mithilfe komplexer Berechnungen ein

Vergleich der Konzepte zur Gewährleistung der Rechtmäßigkeit der Transaktionen

Grafik V.3



Ein Käufer erwirbt eine Ware, wobei der Verkäufer die Lieferung veranlasst, sobald die Zahlung als getätigt anzusehen ist. Bei Überweisung via Bankkonto – d.h. bei zentraler Datenverwaltung (links) – erteilt der Käufer seiner Bank einen Zahlungsauftrag, worauf die Bank den Kontostand entsprechend anpasst (Sollbuchung auf dem Verkäuferkonto, Habenbuchung auf dem Käuferkonto). Daraufhin erhält der Verkäufer eine Zahlungsbestätigung von der Bank. Zahlt der Käufer hingegen in Kryptowährung (rechts), erteilt er zunächst einen allgemein nachvollziehbaren Zahlungsauftrag, wonach das Kryptowährungsguthaben des Käufers um 1 zu reduzieren und jenes des Verkäufers um 1 zu erhöhen ist. Danach aktualisiert ein Miner die Transaktionshistorie entsprechend. Daraufhin übernehmen alle anderen Miner und Nutzer den aktualisierten Stand, indem sie bestätigen, dass mit dem neu erfassten Zahlungsauftrag kein Versuch unternommen wurde, einen Betrag doppelt auszugeben, und dass die Transaktion vom Käufer autorisiert wurde. Für den Verkäufer wird so ersichtlich, dass die Zahlung vom Netzwerk der Miner und Nutzer akzeptiert wurde.

Quelle: Nach R. Auer, „The mechanics of decentralised trust in Bitcoin and the blockchain", *BIS Working Papers*, erscheint demnächst.

bestimmtes Resultat zutage zu befördern, was die Rollenbezeichnung der Miner erklärt.[19] Als Gegenleistung für ihre „Schürfarbeit" erhalten die Miner Transaktionsgebühren von den Nutzern – und falls das Protokoll es so vorsieht, auch neu geschöpfte Kryptowährung.

Zweitens ist die Transaktionshistorie nach jeder Aktualisierung von allen Minern und Nutzern zu validieren, wodurch die Miner wiederum animiert werden, nur rechtmäßige Transaktionen zu berücksichtigen. Rechtmäßig ist hier so zu verstehen, dass die Transaktion vom Geldinhaber ausging und dass kein Versuch unternommen wurde, einen Betrag doppelt auszugeben. Im gegenteiligen Fall wird die Änderung vom Netzwerk nicht akzeptiert und die Vergütung für den Miner (Miner's Reward) wird annulliert. Weil dies nicht im Interesse der Miner ist, sind sie bemüht, nur rechtmäßige Transaktionen hinzuzufügen.[20]

Drittens enthält das Protokoll Konsensmechanismen zur Bestimmung der Reihenfolge, in der die Transaktionshistorie zu aktualisieren ist. Generell funktioniert dies über die Schaffung von Anreizmechanismen für einzelne Miner, bei der Aktualisierung der Mehrheit im System zu folgen. Wichtig ist eine solche Abstimmung zum Beispiel, wenn Kommunikationsverzögerungen dazu führen, dass verschiedene Miner gegenläufige Updates durchführen – d.h. unterschiedliche Transaktionsstränge erfassen (Kasten V.A).

Diese Kernkomponenten machen das Fälschen einer Kryptowährung teuer – jedoch nicht unmöglich. Um einen Betrag zweimal auszugeben, müsste ein Fälscher regulär mit Kryptowährung bezahlen und gleichzeitig im Geheimen eine gefälschte Blockchain ohne die erste Transaktion generieren. Bei Erhalt der Ware würde der Fälscher die gefälschte Blockchain freigeben, d.h. die Zahlung rückgängig machen. Diese gefälschte Blockchain müsste allerdings länger als die vom Rest des Miner-Netzwerks in der Zwischenzeit generierte Blockchain sein, um allseits akzeptiert zu werden. Das heißt, ein Duplizierungsangriff kann nur dann erfolgreich sein, wenn der Angreifer Kontrolle über einen substanziellen Teil der Rechenleistung aller Miner insgesamt hat. Anders gesagt und wie im originären Bitcoin-Weißbuch dargestellt, ist dem Duplizierungsproblem bei einer Kryptowährung dezentral nur dadurch beizukommen, indem „die Rechenleistung überwiegend von ehrlichen Nodes erbracht wird".[21]

Wo liegen die ökonomischen Grenzen von Kryptowährungen, die nicht auf Berechtigungsbasis funktionieren?

Kryptowährungen wie Bitcoin beanspruchen für sich, nicht nur ein praktisches digitales Zahlungsmittel zu sein, sondern auch die Vertrauensbildung, auf die es beim Geld ankommt, auf eine neue Art und Weise zu bewerkstelligen. Dies ist allerdings nur unter der Annahme zu schaffen, dass der überwiegende Teil der Rechenleistung von ehrlichen Minern kontrolliert wird, dass alle Nutzer die komplette Transaktionshistorie validieren und dass die Geldmenge im Protokoll vorgegeben ist. Es ist wichtig, diese Annahmen zu verstehen, denn daraus lassen sich zwei grundlegende Fragen bezüglich der Zweckmäßigkeit von Kryptowährungen ableiten. Erstens: Geht dieser komplexe Vertrauensbildungsprozess auf Kosten der Effizienz? Zweitens: Kann absolutes Vertrauen in die Technologie hinter den Kryptowährungen erreicht werden?

Wie die erste Frage schon impliziert, stößt der enorme Aufwand für die dezentrale Vertrauensbildung irgendwann an Effizienzgrenzen. Es ist davon auszugehen, dass die Miner beim Fortschreiben der Transaktionshistorie so lange miteinander konkurrieren, bis der erhoffte Gewinn gegen null geht.[22] Die Kapazität einzelner von Minern betriebener Rechenzentren kann der Leistung von Millionen von PCs entsprechen. Aktuell ist der gesamte Strombedarf von Bitcoin vergleichbar mit dem Strombedarf mittelgroßer Volkswirtschaften wie der Schweiz, und auch andere Kryptowährungen haben einen hohen Strombedarf (Grafik V.4 links). Auf den Punkt gebracht: Das Streben nach dezentraler Vertrauensbildung hat schnell zu einem Umweltdesaster geführt.[23]

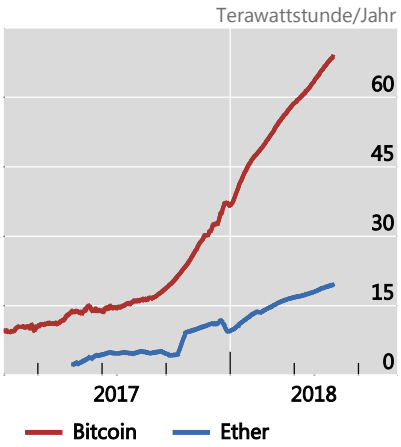
Die grundlegenden ökonomischen Probleme gehen aber weit über die Energieproblematik hinaus. Sie hängen mit der ureigensten Eigenschaft von Geld zusammen, nämlich Netzwerk-Effekte unter den Nutzern zu begünstigen und so als Koordinationsinstrument zu fungieren. In dieser Hinsicht sind Kryptowährungen in dreifacher Weise problematisch, nämlich im Hinblick auf die Skalierbarkeit, die Werthaltigkeit und das Vertrauen in die Finalität der Zahlungen.

Zunächst sind Kryptowährungen nicht wie von staatlichen Stellen ausgegebene Währungen skalierbar. Auf der fundamentalsten Ebene steht und fällt das Versprechen der dezentralen Vertrauensbildung von Kryptowährungen damit, dass jeder einzelne Nutzer die komplette Transaktionshistorie (Zahlungsbetrag, Zahlungserbringer, Zahlungsempfänger etc.) herunterladen und validieren muss. Da jede Transaktion mit ein paar hundert Bytes zu Buche schlägt, wächst das Datenvolumen im Lauf der Zeit sehr stark an. So wächst die Bitcoin-Blockchain derzeit um rund

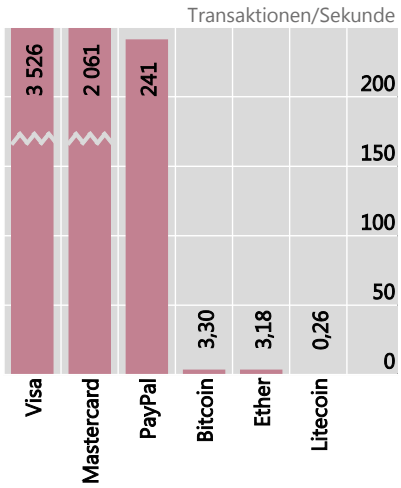
Energieverbrauch und Skalierungsproblem

Grafik V.4

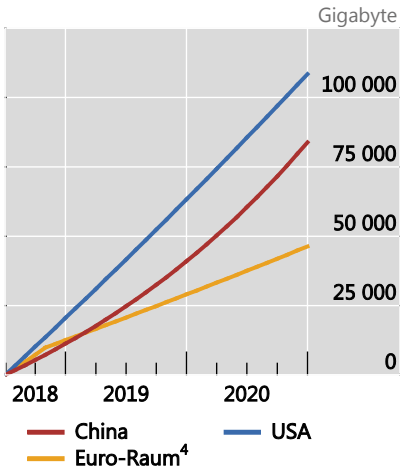
Energieverbrauch ausgewählter Kryptowährungen[1]



Zahl der Transaktionen je Sekunde[2]



Hypothetische Datengröße bei Abwicklung des Massenzahlungsverkehrs mit Kryptowährungen[3]



[1] Geschätzt. [2] Angaben für 2017. [3] Die dargestellte hypothetische Größe der Blockchain/der Transaktionshistorie beruht auf der Annahme, dass ab 1. Juli 2018 der gesamte bargeldlose Massenzahlungsverkehr in China, den USA und im Euro-Raum in Kryptowährungen abgewickelt wird. Die Berechnungen basieren auf den Daten zum bargeldlosen Zahlungsverkehr laut CPMI (2017) und der Annahme, dass sich der Datenbestand mit jeder Transaktion um 250 Byte erhöht. [4] BE, FR, DE, IT und NL.

Quellen: Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (CPMI), *Statistics on payment, clearing and settlement systems in the CPMI countries*, Dezember 2017; www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa; Berechnungen der BIZ.

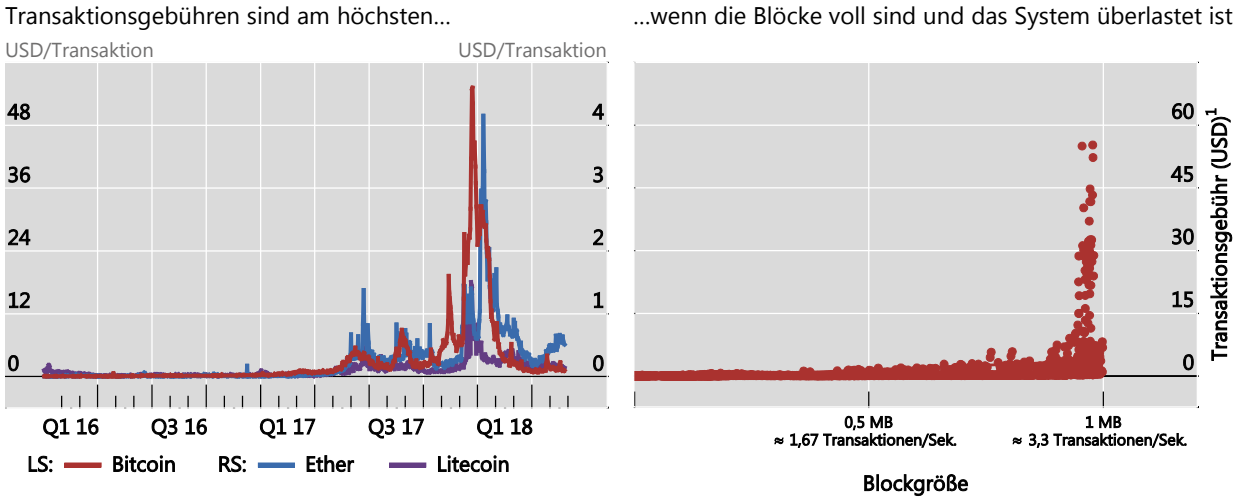
50 Gigabyte pro Jahr, wobei sie aktuell etwa 170 Gigabyte ausmacht. Damit also das Datenvolumen und die zur Validierung aller Transaktionen erforderliche Zeit (die mit jedem Block zunimmt) im Rahmen bleiben, gelten für den Durchsatz von Transaktionen strenge Obergrenzen (Grafik V.4 Mitte).

Ein Gedankenexperiment stellt die Alltagstauglichkeit von Kryptowährungen infrage (Grafik V.4 rechts). Um die Anzahl digitaler Transaktionen im Massenzahlungsverkehr, die aktuell im Zahlungsverkehr bestimmter Volkswirtschaften bewältigt werden, verarbeiten zu können, würde der Datenbestand auch bei optimistischen Annahmen binnen weniger Tage die Speicherkapazität gängiger Smartphones, binnen weniger Wochen die Kapazität von PCs und binnen weniger Monate auch die Kapazitäten ganzer Server übersteigen. Aber nicht nur die Speicherkapazität, auch die Verarbeitungskapazität ist ein Problem: Nur Supercomputer könnten die eingehenden Zahlungsaufträge validieren. Die damit zusammenhängenden Kommunikationsvolumina könnten das Internet lahmlegen, wenn Millionen von Nutzern Dateien in der Größenordnung von einem Terabyte austauschen.

Ein weiterer Aspekt der Skalierbarkeit ist die Stauanfälligkeit der Ledger-Aktualisierung. Damit nicht zu viele neue Transaktionen auf einmal erfasst werden, lassen sich bei Kryptowährungen auf Blockchain-Basis neue Blöcke nur in vordefinierten Intervallen anhängen. Summieren sich die eingehenden Zahlungsaufträge derart, dass der laut Protokoll zulässige Höchstwert erreicht ist, bildet sich ein Stau, und viele Transaktionen landen in der Warteschleife. Bei Erreichen des Kapazitätslimits schnellen die Gebühren nach oben (Grafik V.5), und Transaktionen können bis zur Abwicklung stundenlang in der Warteschleife hängen. Damit sind Kryptowährungen im Alltag, etwa zum Bezahlen eines Kaffees oder einer Konferenzgebühr, nur begrenzt

Entwicklung der Transaktionsgebühren im Zeitverlauf und in Relation zum Durchsatz

Grafik V.5



[1] An Miner im Zeitraum 1. August 2010–25. Mai 2018 entrichtete Transaktionsgebühren; Tagesdurchschnitte.

Quellen: www.bitinfocharts.com; Berechnungen der BIZ.

einsetzbar, vom Großbetragszahlungsverkehr ganz zu schweigen.[24] Je populärer eine Kryptowährung also wird, desto umständlicher wird das Zahlen damit – es tritt also genau das Gegenteil dessen ein, was eine wesentliche Eigenschaft des Geldes heute ausmacht: Je mehr Menschen es nutzen, desto höher der Anreiz, dies ebenso zu tun.[25]

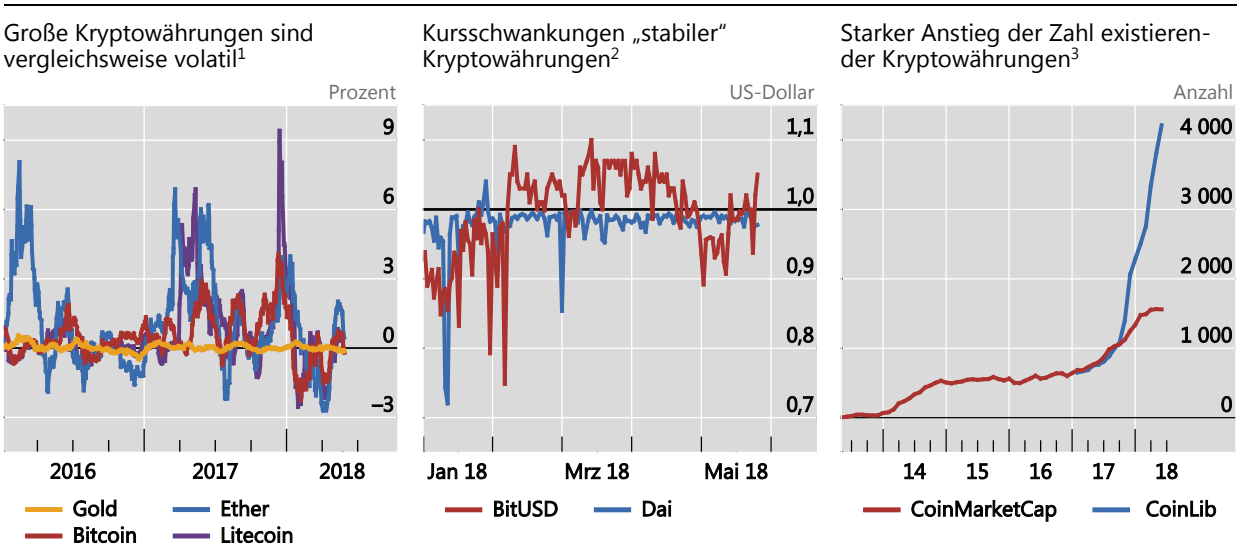
Neben der Skalierbarkeit ist auch die Kursinstabilität von Kryptowährungen problematisch. Diese ergibt sich daraus, dass es keine zentrale ausgebende Stelle mit einem Stabilitätsauftrag gibt. Gut funktionierende Zentralbanken können den Innenwert der Landeswährung stabil halten, indem sie je nach Transaktionsnachfrage mehr oder weniger Zahlungsmittel zur Verfügung stellen. An dieser Schraube dreht die Zentralbank immer wieder, insbesondere bei Marktanspannungen, aber auch in normalen Zeiten.

Bei Kryptowährungen hingegen muss die Geldmenge durch das Protokoll vorgegeben sein, denn nur so lässt sich das Vertrauen in ihren Kurs aufbauen. Damit kann die Geldmenge aber nicht elastisch angepasst werden, was wiederum zur Folge hat, dass sich Nachfrageschwankungen in Kursschwankungen niederschlagen. Deshalb sind die Kryptowährungskurse äußerst volatil (Grafik V.6 links). Bessere Protokolle oder Financial Engineering – man denke an die Erfahrung mit der Kryptowährung „Dai" – dürften das Problem der inhärenten Instabilität kaum lösen. So rutschte der Dai-Kurs trotz einer 1:1-Bindung an den US-Dollar binnen weniger Wochen nach seiner Einführung Ende 2017 auf einen Wert von $ 0,72. Substanzielle Fluktuationen waren aber auch bei anderen, auf Kursstabilität ausgelegten Kryptowährungen zu beobachten (Grafik V.6 Mitte).

Kursinstabilität bei Kryptowährungen ist kein Zufall. Um die Geldmenge an die Transaktionsnachfrage anpassen zu können, braucht es eine zentrale Instanz, typischerweise die Zentralbank, die imstande ist, ihre Bilanz zu verlängern oder zu verkürzen. Diese Instanz muss zudem gewillt sein, sich gegebenenfalls gegen den Markt zu stellen, auch wenn sie zu diesem Zweck Bilanzrisiken eingehen und Verluste

Volatilität ausgewählter Kryptowährungen und Anzahl von Kryptowährungen

Grafik V.6



[1] Gleitender 30-Tage-Durchschnitt der Tageserträge. [2] Niedrigster Tageskurs. [3] Basierend auf Monatsangaben der zwei genannten Anbieter, wobei CoinMarketCap Kryptowährungen erst ab einem Mindestumsatz von $ 100 000 innerhalb von 24 Stunden erfasst, CoinLib hingegen unbegrenzt.

Quellen: www.bitinfocharts.com; www.coinlib.io; www.coinmarketcap.com; Datastream.

in Kauf nehmen muss. In einem dezentralen Netzwerk aus Kryptowährungsteilnehmern gibt es keine zentrale Instanz, die die Verpflichtung oder den Anreiz zur Kursstabilisierung hat: Bei sinkender Nachfrage nach einer Kryptowährung fällt also auch ihr Kurs.

Zur Kursinstabilität trägt auch die Geschwindigkeit bei, mit der neue Kryptowährungen entstehen. Aktuell gibt es einige Tausend Kryptowährungen, wobei zuverlässige Schätzungen zur Zahl existierender Kryptowährungen schwierig sind (Grafik V.6 rechts). Wie die in der Vergangenheit mit Privatbanken gemachten Erfahrungen zeigen, führt eine liberale Ausgabe neuen Geldes selten zu Stabilität.

Problematisch ist schließlich auch die fragile Vertrauensbasis von Kryptowährungen. Dies betrifft sowohl die Finalität einzelner Zahlungen als auch den Kurs einzelner Kryptowährungen.

Im herkömmlichen Zahlungsverkehr gilt, dass eine bestimmte Zahlung nicht widerrufen werden kann, sobald sie das nationale Zahlungsverkehrssystem durchlaufen hat und letztlich zentralbankseitig erfasst wurde. Kryptowährungen hingegen, die nicht auf Berechtigungsbasis funktionieren, können die Finalität einzelner Zahlungen nicht gewährleisten. Dies liegt u.a. daran, dass Nutzer zwar die Abbildung einer bestimmten Transaktion in der Transaktionshistorie validieren können, aber nicht auszuschließen ist, dass es rivalisierende Versionen der Transaktionshistorie gibt. Dies kann dazu führen, dass eine Transaktion rückabgewickelt wird, etwa wenn die Historie von zwei Minern nahezu zeitgleich aktualisiert wird. Da letztlich nur eine Version übrigbleiben kann, ist die Finalität parallel erfasster Zahlungen eine Wahrscheinlichkeitsfrage.

Die fehlende Zahlungsfinalität ist umso problematischer, als Kryptowährungen durch Miner mit Kontrolle über eine substanzielle Rechenleistung manipulierbar sind. Angesichts der Konzentration der Rechenleistung auf nur wenige Miner ist eine

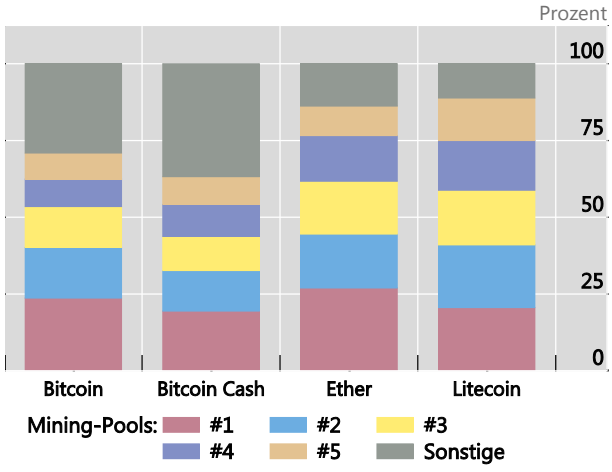
derartige Manipulation eine reale Gefahr (Grafik V.7 links). Strategische Angriffe sind nicht erkennbar, weil eine gefälschte Transaktionshistorie nur dann publik gemacht würde, wenn der Angreifer sich seines Erfolges sicher ist. Damit bleibt die Finalität immer ein offener Punkt. Kryptowährungen sind so konzipiert, dass jede Aktualisierung der Transaktionshistorie eine zusätzliche Rechenleistung erfordert, die der Angreifer reproduzieren müsste. Mit anderen Worten: Die Wahrscheinlichkeit, dass eine Zahlung final ist, steigt zwar mit der Zahl der danach erfassten Zahlungen, aber sie wird nie 100% erreichen.[26]

Fraglich ist allerdings nicht nur das Vertrauen in eine einzelne Zahlung, auch das Vertrauen in Kryptowährungen an sich ist fragil. Der Grund dafür liegt in sog. Aufspaltungen (Forking). Damit ist ein Prozess gemeint, in dem ein Teil der Kryptowährungsbesitzer sich auf die Verwendung einer neuen Version zur Transaktionserfassung bzw. einer neuen Protokollversion verständigt, während andere bei der Originalversion bleiben. So kann sich eine Kryptowährung-Community in zwei Teilnetzwerke aufspalten. Dafür ließen sich zahlreiche aktuelle Beispiele anführen. Bemerkenswert ist in diesem Zusammenhang jedoch eine Episode vom 11. März 2013, als – im Widerspruch zur vielzietierten vertrauensbildenden Wirkung dezentraler Strukturen – durch zentrale Koordination der Miner die Aufspaltung rückgängig gemacht wurde. Damals führte ein falsches Softwareupdate zu Inkompatibilitäten zwischen zwei Teilen des Bitcoin-Netzwerks, die Mining auf Basis des alten Protokolls bzw. auf Basis des aktualisierten Protokolls betrieben. Dadurch wuchsen einige Stunden lang zwei separate Blockchains, und der Bitcoin-Kurs brach bei Bekanntwerden dieser Aufspaltung um nahezu ein Drittel ein (Grafik V.7 rechts). Diese Aufspaltung wurde letztlich in einer konzertierten Aktion rückgängig gemacht, wobei die Miner vorübergehend vom Protokoll abwichen und die längste Kette ignorierten. Allerdings wurde eine hohe Zahl von Transaktionen Stunden, nachdem Nutzer sie final geglaubt hatten, ungültig. Diese Episode zeigt, wie einfach es zu einer

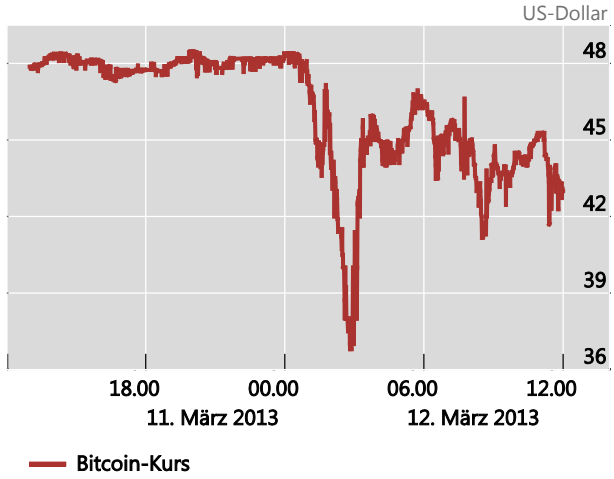
Mining-Konzentration und Bitcoin-Kursentwicklung bei temporärer Aufspaltung

Grafik V.7

Mining vieler Kryptowährungen ist konzentriert[1]



Entwicklung des Bitcoin-Kurses im Zuge einer temporären Aufspaltung 2013[2]



[1] Angaben beziehen sich auf die größten Mining-Pools zum Stichtag 28. Mai 2018. [2] Bitcoin-Kursentwicklung während der Bitcoin-Aufspaltung am 11./12. März 2013.

Quellen: www.btc.com; www.cash.coin.dance; CoinDesk; www.etherchain.org; www.litecoinpool.org.

Aufspaltung von Kryptowährungen mit entsprechend hohen Kursverlusten kommen kann.

Weit besorgniserregender ist jedoch der Gedanke, dass derartige Aufspaltungen nur symptomatisch für ein grundlegendes Problem sein könnten, nämlich die Fragilität des dezentralen Konsenses für die Fortschreibung der Transaktionshistorie – und damit zusammenhängend die Fragilität des grundsätzlichen Vertrauens in die Kryptowährung. Eine theoretische Analyse (Kasten V.A) legt nahe, dass die Koordinierung der Art und Weise, wie die Transaktionshistorie fortzuschreiben ist, jederzeit zusammenbrechen und zu einem Totalverlust führen könnte.

Insgesamt leiden dezentrale Kryptowährungen an einer Reihe von Mängeln, wobei sich die größten Ineffizienzen aus dem extrem hohen Dezentralisierungsgrad ergeben: In einem solchen Rahmen für die nötige Vertrauensbildung zu sorgen bedeutet eine enorme Verschwendung von Rechenleistung, die dezentrale Datenverwaltung ist ineffizient, und der dezentrale Konsens ist fragil. Einige dieser Probleme ließen sich mit neuartigen Protokollen und weiteren Verbesserungen in den Griff bekommen.[27] Andere Probleme scheinen aber inhärent mit der Fragilität und der begrenzten Skalierbarkeit derartiger dezentraler Systeme zusammenzuhängen. Letztlich legt dies nahe, dass das Fehlen einer adäquaten institutionellen Absicherung auf der nationalen Ebene das grundlegendste Problem darstellt.

Andere Anwendungsbereiche für die Distributed-Ledger-Technologie

Während Kryptowährungen als Geld nicht funktionieren, dürfte die ihnen zugrundeliegende Technologie in anderen Bereichen vielversprechend sein. Ganz allgemein kann die Distributed-Ledger-Technologie verglichen mit herkömmlichen zentralisierten technischen Lösungen in Nischenbereichen effizient sein, weil dort die Vorteile eines dezentralen Zugangs die höheren Betriebskosten aufgrund der vielfachen parallelen Datenspeicherung wettmachen.

Ein aktuelles Bespiel aus dem Non-Profit-Bereich ist das „Building Blocks"-System des Welternährungsprogramms, über das die Lebensmittelhilfe für syrische Flüchtlinge in Jordanien auf Blockchain-Basis abgerechnet wird. Recheneinheit und eigentliches Zahlungsmittel bei Building Blocks ist die offizielle Währung, d.h., es handelt sich dabei um ein Kryptozahlungssystem und nicht um eine Kryptowährung. Außerdem gibt es mit dem Welternährungsprogramm eine zentrale Kontrollinstanz, und dies aus gutem Grund: Ein erstes Experiment mit dem Ethereum-Protokoll ohne Berechtigungssystem führte zu schleppenden und kostspieligen Transaktionen. Das System wurde danach auf eine Version des Ethereum-Protokolls auf Berechtigungsbasis umgestellt. So ließen sich die Transaktionskosten gegenüber den bankbasierten Alternativen um etwa 98% verringern.[28]

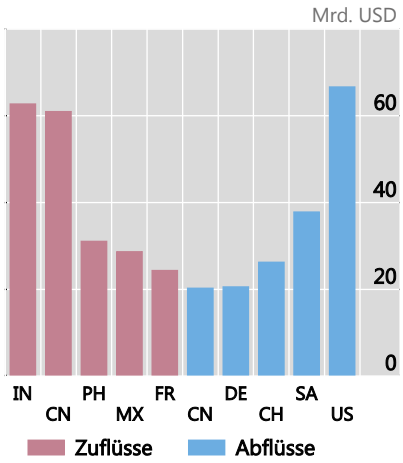
Kryptozahlungssysteme auf Berechtigungsbasis könnten auch für kleine Geldtransfers ins Ausland vielversprechend sein, was für Länder eine Rolle spielt, deren Erwerbsbevölkerung zu einem hohen Teil im Ausland lebt. Derzeit übersteigen Auslandsüberweisungen weltweit jährlich $ 540 Mrd. (Grafik V.8 links und Mitte), wobei die Abwicklung jeweils über mehrere Intermediäre läuft, mit entsprechend hohen Kosten (Grafik V.8 rechts). Allerdings sind Kryptozahlungsverkehrssysteme nicht die einzige Option, die Kosten in diesem Marktsegment senken könnte, und es ist noch nicht absehbar, welche Technologie sich als die effizienteste herauskristallisieren wird.

Umsatz- und Kostenkennzahlen für Überweisungen

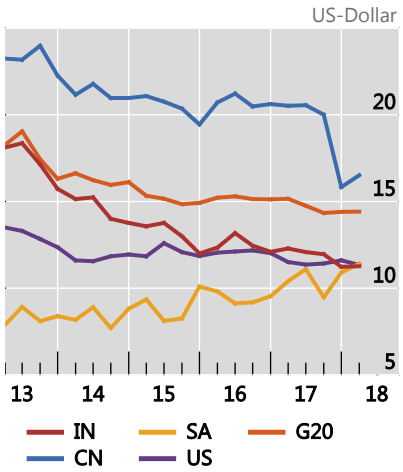
Grafik V.8

Überweisungsumsätze tendenziell steigend, daher…

…viele Kleinbetragszahlungen zwischen oft illiquiden Währungspaaren…[1]



…zu hohen Durchschnittskosten[2]



[1] Angaben für 2016. [2] Gesamtkosten für eine Überweisung von $ 200 (Durchschnitt aller Anbieter weltweit). CN und IN: Durchschnittkosten auf Empfängerseite; G20, SA und US: Durchschnittskosten auf Senderseite.

Quellen: *Remittance Prices Worldwide* der Weltbank (remittanceprices.worldbank.org); Weltbank; Berechnungen der BIZ.

Eine wichtigere Rolle dürften Anwendungen spielen, die den Kryptozahlungsverkehr mit komplexen, automatisierten Programmcodes und Datenzugangssystemen kombinieren. Bereits heute können auf Basis dezentraler Kryptowährungsprotokolle wie Ethereum „intelligente Verträge" (Smart Contracts) verarbeitet werden, die für die automatisierte Abwicklung des Zahlungsverkehrs im Derivathandel sorgen. In der Wirksamkeit sind diese Produkte derzeit aufgrund der geringen Liquidität und der intrinsischen Ineffizienzen von Kryptowährungen ohne Berechtigungssystem begrenzt. Die zugrundeliegende Technologie kann aber im Börsenhandel auf Basis von Berechtigungsprotokollen und mit herkömmlichem Geld als Deckungsstock verwendet werden, wodurch sich der Abwicklungsprozess vereinfacht. Der Mehrwert der Technologie dürfte sich aus der Vereinfachung der Abwicklung komplexer Finanztransaktionen, wie der Handelsfinanzierung (Kasten V.B), ergeben. Wichtig ist jedoch, dass keine dieser Anwendungen die Verwendung von Kryptowährungen erfordert.

Implikationen für die Politik

Der Vormarsch der Kryptowährungen und der damit verbundenen Technologie wirft eine Reihe politischer Fragen auf. Für die Behörden stehen grundsätzlich die Gewährleistung der Markt- und Zahlungsverkehrsintegrität, der Konsumenten- und Anlegerschutz und insgesamt die Wahrung der Finanzstabilität im Zentrum. Eine wichtige Herausforderung ist in diesem Zusammenhang der Kampf gegen illegale Geldflüsse. Zugleich wollen die Behörden langfristige Innovationsanreize bewahren und insbesondere am Prinzip „gleiche Risiken, gleiche Regeln" festhalten.[29] Diese Ziele sind nicht grundsätzlich neu, aber mit den Kryptowährungen sind neue Herausforderungen aufgetaucht, die eventuell für neue Instrumente und Ansätze sprechen.

Damit zusammenhängend stellt sich auch die Frage, ob Zentralbanken selber Digitalgeld ausgeben sollten.

Regulatorische Herausforderungen durch Kryptowährungen

Als erste regulatorische Herausforderung ist die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu nennen. Hier stellt sich die Frage, inwieweit der Vormarsch der Kryptowährungen dazu geführt hat, dass die diesbezüglichen Maßnahmen (wie Kundenidentifizierungsstandards) umgangen werden. Da Kryptowährungen anonym sind, lässt sich schwer feststellen, inwieweit sie für illegale Transaktionen verwendet werden oder auch, um Kapitalverkehrskontrollen oder Steuergesetze zu umgehen. Allerdings sprechen Ereignisse wie die starke Marktreaktion des Bitcoin-Kurses auf die Schließung von Silk Road, einem großen Umschlagplatz für illegale Drogen, dafür, dass ein nicht unbedeutender Teil der Nachfrage nach Kryptowährungen im Zusammenhang mit illegalen Aktivitäten steht (Grafik V.9 links).[30]

Zweitens sind Kryptowährungen ein Thema im Zusammenhang mit Wertpapierbestimmungen sowie anderen Konsumenten- und Anlegerschutzbestimmungen. Ein gängiges Problem ist digitaler Diebstahl. Da Kryptowährungen aufgrund ihres technischen Konzepts sehr viel Speicherplatz benötigen und hohe Transaktionskosten mit sich bringen, haben Privatanleger meist nur über Intermediäre (Anbieter von Kryptowallets oder Kryptobörsen) Zugang zu ihren Kryptoguthaben. Paradoxerweise – und entgegen dem ursprünglichen Anspruch von Bitcoin und anderen Kryptowährungen – finden sich viele Nutzer, die sich aus Misstrauen gegenüber der Notenbank bzw. dem Staat für Kryptowährungen entschieden hatten, in der Situation wieder, von unregulierten Intermediären abhängig zu sein. Einige dieser Intermediäre (wie Mt Gox oder Bitfinex) haben sich als Betrüger erwiesen oder wurden selbst Opfer von Hackerattacken.[31]

Von Betrugsfällen betroffen sind auch Neuemissionen von Kryptowährungen (Initial Coin Offerings, ICOs). ICOs sind Finanzierungslösungen, die über die Ausgabe neuer Kryptowährungen auf Tenderbasis funktionieren, wobei Anleger teilweise auch Beteiligungen (etwa an Startups) erwerben können. Trotz Behördenwarnungen und obwohl die Unternehmensprojekte meist undurchschaubar und kaum dokumentiert sind, finden ICOs bei Investoren regen Zuspruch. Viele durch ICOs finanzierte Projekte haben sich nach nur kurzer Zeit als betrügerische Pyramidenspiele erwiesen (Grafik V.9 rechts).

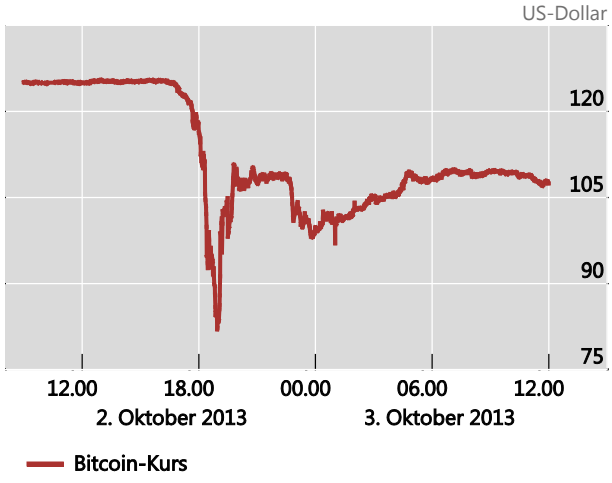
Die dritte regulatorische Herausforderung besteht auf längere Sicht im Zusammenhang mit der Stabilität des Finanzsystems. Es bleibt abzuwarten, ob die weitverbreitete Nutzung von Kryptowährungen und damit verbundenen Finanzprodukten auf Basis intelligenter Verträge das Finanzsystem auf neue Weise verwundbar machen und neue systemische Risiken heraufbeschwören. Wichtig ist, die Entwicklungen genau zu beobachten. Weil das Risikoprofil neu ist, sind die Regulierungs- und Aufsichtsinstanzen zudem gefordert, mit den technologischen Entwicklungen Schritt zu halten. In bestimmten Bereichen, etwa bei Großbetragszahlungen, dürfte es notwendig werden, Unternehmen, die die neuen Technologien nutzen, ebenfalls der Aufsicht zu unterstellen, um den Aufbau systemischer Risiken zu verhindern.

Die Notwendigkeit strengerer oder neuer regulatorischer Bestimmungen und der Überwachung von Kryptowährungen und Kryptoanlagen wurde gemeinhin auf

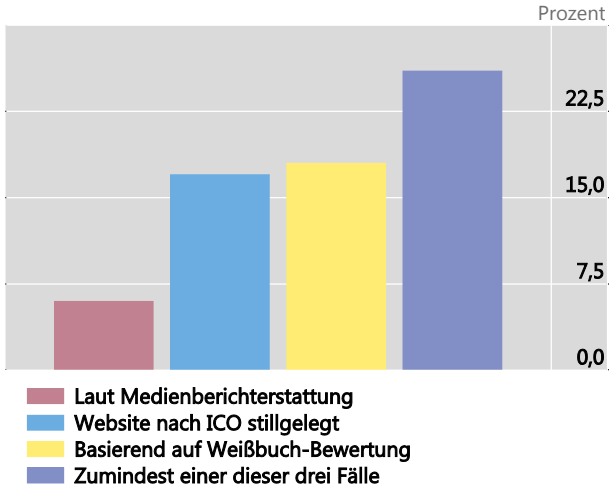
Schließung eines illegalen Marktplatzes und Legitimität von ICOs

Grafik V.9

Starke Reaktion von Kryptowährungskursen auf Schließung illegaler Marktplätze[1]



ICOs sind vermutlich oft Betrugsfälle



[1] Bitcoin-Kursentwicklung im Zuge der Schließung von Silk Road im Oktober 2013.

Quellen: C. Catalini, J. Boslego und K. Zhang, „Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, erscheint demnächst; CoinDesk.

regulatorischer Ebene weltweit erkannt. So haben die Finanzminister und Zentralbankpräsidenten der G20 kürzlich in einem Communiqué Fragen des Konsumenten- und Anlegerschutzes, der Marktintegrität, der Steuerflucht sowie der Geldwäsche und Terrorismusfinanzierung thematisiert und die Wichtigkeit der lückenlosen Überwachung auf Basis internationaler Standards und der diesbezüglichen Gremienarbeit unterstrichen. In diesem Sinn erging auch ein Appell an die Financial Action Task Force, die Umsetzung der geltenden Standards weltweit voranzutreiben.[32]

Allerdings sind sowohl die Ausgestaltung als auch die effektive Umsetzung strengerer Standards schwierig. Die rechtlichen und regulatorischen Definitionen entsprechen nicht immer den neuen digitalen Realitäten. Dieselben Technologien werden für diverse wirtschaftliche Aktivitäten verwendet, die vielfach von unterschiedlichen Behörden reguliert werden. So werden ICOs aktuell von Technologiefirmen zur Finanzierung von Projekten genutzt, die mit Kryptowährungen nichts zu tun haben. Faktisch unterscheiden sich ICOs nicht vom herkömmlichen Börsengang (Initial Public Offerings, IPOs), weshalb es naheliegen würde, bei der Regulierung und Beaufsichtigung gleiche Maßstäbe anzulegen. Allerdings versprechen manche ICOs einen bestimmten Nutzwert (Utility Tokens), wie etwa den Zugang zu künftigen Softwareprodukten (z.B. Spielen). Dieser Aspekt hat aber nichts mit einer Anlagetätigkeit zu tun, sondern fällt unter das Konsumentenschutzgesetz und damit in die Zuständigkeit der relevanten Gremien.[33]

Der regulatorische Ansatz wird dadurch verkompliziert, dass Kryptowährungen ohne Berechtigungssystem nicht ohne Weiteres in den existierenden regulatorischen Rahmen passen. So gibt es keine Rechtspersönlichkeit, auf die die regulatorischen Bestimmungen anzuwenden wären. Kryptowährungen existieren in ihrem eigenen digitalen, staatenlosen Umfeld und können weitgehend isoliert von bestehenden institutionellen Rahmenbedingungen oder sonstigen Infrastrukturen funktionieren. Ihr Sitz – soweit es einen gibt – kann sich im Ausland befinden oder womöglich nicht eindeutig bestimmbar sein. Somit können sie nur indirekt reguliert werden.

Wie können die Regulierungs- und Aufsichtsinstanzen aktiv werden? Diesbezüglich sind drei Überlegungen relevant.

Erstens verlangt der Vormarsch der Kryptowährungen und Kryptoanlagen danach, die regulatorischen Grenzen neu zu ziehen und sie an die neue Realität anzupassen, in der sich die Grenzen zwischen den Zuständigkeiten der einzelnen nationalen und internationalen Regulatoren zunehmend verwischen.[34] Da die Kryptowährungen an sich global sind, lassen sie sich nur mit global abgestimmten Maßnahmen wirksam regeln.[35]

Zweitens kann die Regulierung an den Schnittstellen zwischen den Kryptowährungen und regulierten Finanzinstituten ansetzen. Nur regulierte Börsen können die Liquidität aufbringen, die es braucht, damit Kryptowährungen und auf ihnen aufbauende Finanzprodukte keine Nischenprodukte bleiben, und die Abwicklungssummen müssen letztlich in eine offizielle Währung konvertiert werden. Die Steuergesetze und die Eigenkapitalvorschriften für regulierte Institute, die mit Anlagen im Stil von Kryptowährungen handeln wollen, könnten angepasst werden. Die Regulierung könnte ferner überwachen, ob und wie Banken Kryptowährungen als Sicherheiten hinterlegen oder erhalten.

Drittens kann die Regulierung Institutionen, die kryptowährungsspezifische Dienstleistungen erbringen, ins Visier nehmen. Um etwa die Wirksamkeit der Bestimmungen gegen Geldwäsche und Terrorismusfinanzierung sicherzustellen, könnte die Regulierung an dem Punkt ansetzen, an dem eine Kryptowährung in eine offizielle Währung konvertiert wird. Andere bestehende gesetzliche und regulatorische Vorschriften fokussieren auf Sicherheit, Effizienz und Rechtmäßigkeit. Diese Prinzipien sind auch auf Firmen anwendbar, die die Infrastruktur für Kryptowährungen anbieten, wie Kryptowallets.[36] Um Schlupflöcher zu vermeiden, sollten die entsprechenden Bestimmungen international harmonisiert sein und konsistent umgesetzt werden.

Sollten Zentralbanken Digitalgeld ausgeben?

In diesem Zusammenhang stellt sich auch eine geldpolitische Frage, die auf mittlere Sicht zu klären sein wird: Sollten Zentralbanken Digitalgeld ausgeben, und wenn ja, wer sollte Zugang dazu haben? Digitales Zentralbankgeld würde weitgehend wie Bargeld funktionieren: Ist es einmal im Umlauf, nach Ausgabe durch die Zentralbank, würde es ohne weitere Involvierung der Zentralbank zwischen den Banken, den Nichtfinanzunternehmen und den Konsumenten zirkulieren.[37] Digitales Zentralbankgeld könnte zwischen privatwirtschaftlichen Akteuren auf Basis der Distributed-Ledger-Technologie bilateral transferiert werden, ohne dass die Zentralbank den Geldfluss nachverfolgen und die Guthaben entsprechend anpassen müsste. Die Basis dafür wäre ein Distributed-Ledger-Konzept auf Berechtigungsbasis (Grafik V.2), wobei die Zentralbank festlegen würde, wer als Trusted Node fungiert.

Die Unterscheidung zwischen generell (d.h. für private Haushalte und Unternehmer) verfügbarem digitalem Zentralbankgeld und herkömmlichen digitalen Zentralbankverbindlichkeiten – den Reserveguthaben der Geschäftsbanken – mag rein technisch erscheinen, aber faktisch besteht ein grundlegender Unterschied bezüglich der Implikationen für das Finanzsystem. Generell verfügbares digitales Zentralbankgeld könnte drei Kernbereiche des Zentralbankwesens tiefgreifend verändern: den Zahlungsverkehr, die Finanzstabilität und die Geldpolitik. Ein gemeinsamer Bericht des Ausschusses für Zahlungsverkehr und Marktinfrastrukturen und des Märkteausschusses bringt die diesbezüglichen Überlegungen auf den Punkt.[38] Der Bericht kommt zu dem Schluss, dass die Stärken und Schwächen von generell

verfügbarem digitalem Zentralbankgeld von dessen konkreter Ausgestaltung abhängen würden. Digitales Zentralbankgeld könnte das Bankensystem anfälliger für Krisen machen, während der Nutzen weniger klar erscheint.

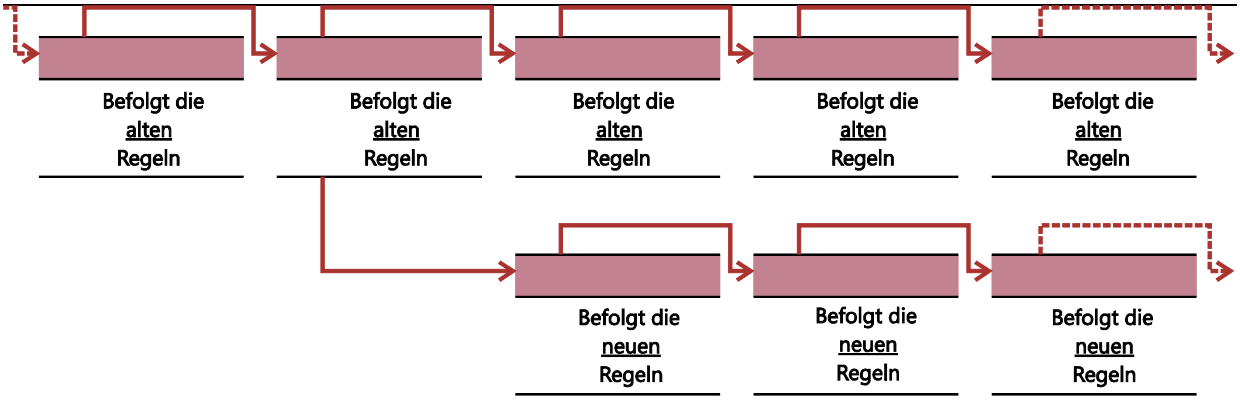
Zentralbanken verfolgen den derzeitigen technologischen Fortschritt genau, agieren aber im Hinblick auf die praktische Umsetzung vorsichtig abwartend. Aktuell evaluieren einzelne Zentralbanken die Vor- und Nachteile der Ausgabe von eingeschränkt verfügbarem digitalem Zentralbankgeld mit Blick auf Großbetragszahlungen im Finanzsektor. Damit würde sich am aktuellen Zweistufenmodell der Geldschöpfung nichts ändern. Sinn und Zweck wäre vielmehr die Verbesserung der operativen Effizienz der bestehenden Strukturen und Prozesse. Die derzeitige Datenlage spricht allerdings nicht eindeutig für eine unmittelbare Versorgung des Finanzsektors mit digitalem Zentralbankgeld (Kasten V.C).

Kasten V.A

Aufspaltungen von Kryptowährungen und Instabilität der dezentralisierten Vertrauensbildung bei Blockchains

Die Zahl der Kryptowährungen ist nicht zuletzt aufgrund von Aufspaltungen, sog. Forks, nach oben geschnellt (Grafik V.6 rechts). Alleine im Monat Januar 2018 wurden die folgenden Aufspaltungen registriert: Bitcoin ALL, Bitcoin Cash Plus, Bitcoin Smart, Bitcoin Interest, Quantum Bitcoin, BitcoinLite, Bitcoin Ore, Bitcoin Private, Bitcoin Atom und Bitcoin Pizza. Zu solchen permanenten oder temporären Aufspaltungen kann es auf unterschiedliche Weise kommen. Eine Möglichkeit sind sog. „harte" Aufspaltungen (Grafik V.A). Dazu kommt es, wenn sich ein Teil der Miner auf neue Regeln im Protokoll verständigt, die nicht mit dem bisherigen Protokoll kompatibel sind. Diese Änderung kann zahlreiche Protokollaspekte betreffen, etwa die maximale Blockgröße, die Häufigkeit, mit der Blöcke zur Blockchain hinzugefügt werden können, oder eine Änderung des zur Aktualisierung der Blockchain erforderlichen Leistungsnachweises. Die auf das neue Protokoll umgestiegenen Miner gehen von der alten Blockchain aus, fügen dann aber Blöcke hinzu, die von den Minern, die nicht umgestiegen sind, nicht anerkannt werden. Letztere bauen weiterhin an der bestehenden Blockchain, die auf den alten Regeln basiert. Dies führt dazu, dass zwei separate Blockchains entstehen, jede Kette mit ihrer eigenen Transaktionshistorie.

Beispiel einer „harten" Aufspaltung — Grafik V.A



Quelle: BIZ.

Häufige Aufspaltungen bei einer Kryptowährung können ein Indiz dafür sein, dass der Konsensmechanismus im dezentralen Netzwerk der Miner ein inhärentes Problem darstellt. Ökonomisch betrachtet ist problematisch, dass dieser dezentrale Konsensmechanismus nicht einzigartig ist. Die Regel, nach der die längste Kette fortzusetzen ist, animiert die Miner, sich nach der Mehrheit im System zu richten – wobei dieser Weg nicht eindeutig vorgegeben ist. Ist ein Miner beispielsweise der Ansicht, dass die letzte Aktualisierung der Transaktionshistorie von den übrigen Minern des Netzwerks ignoriert wird, hat er die Möglichkeit, diese letzte Änderung ebenfalls zu ignorieren. Und stimmt die Mehrheit der Miner darin überein, eine Änderung abzulehnen, so entsteht de facto ein neues Gleichgewicht. Es ist somit möglich, dass willkürliche Gleichgewichte entstehen. Dies ist schon häufig vorgekommen, was sich an den Aufspaltungen und der Existenz von Tausenden sog. Waisen-Blöcke (Bitcoin) und Onkel-Blöcke (Ethereum) zeigt, die inzwischen ungültig geworden sind. Anlass für weitere Bedenken hinsichtlich der Robustheit der dezentralen Blockchain-Aktualisierung geben die Anreize der Miner, strategische Aufspaltungen vorzunehmen, sobald ein von einem anderen Miner hinzugefügter Block mit hohen Transaktionsgebühren verbunden ist. Diese können nämlich umgangen werden, indem der betreffende Block mittels Aufspaltung ungültig gemacht wird.①

① Für eine Analyse der Einzigartigkeit der Aktualisierung der Blockchain siehe B. Biais, C. Bisière, M. Bouvard und C. Casamatta (2017), „The blockchain folk theorem", *TSE Working Papers*, Nr. 17–817. Für eine Analyse der strategischen Gründe für eine Aufspaltung siehe M. Carlsten, H. Kalodner, S. M. Weinberg und A. Narayanan (2016), „On the instability of Bitcoin without the block reward", *Tagungsband der ACM SIGSAC Conference on Computer and Communications Security 2016*.

Kasten V.B

Die Distributed-Ledger-Technologie in der Handelsfinanzierung

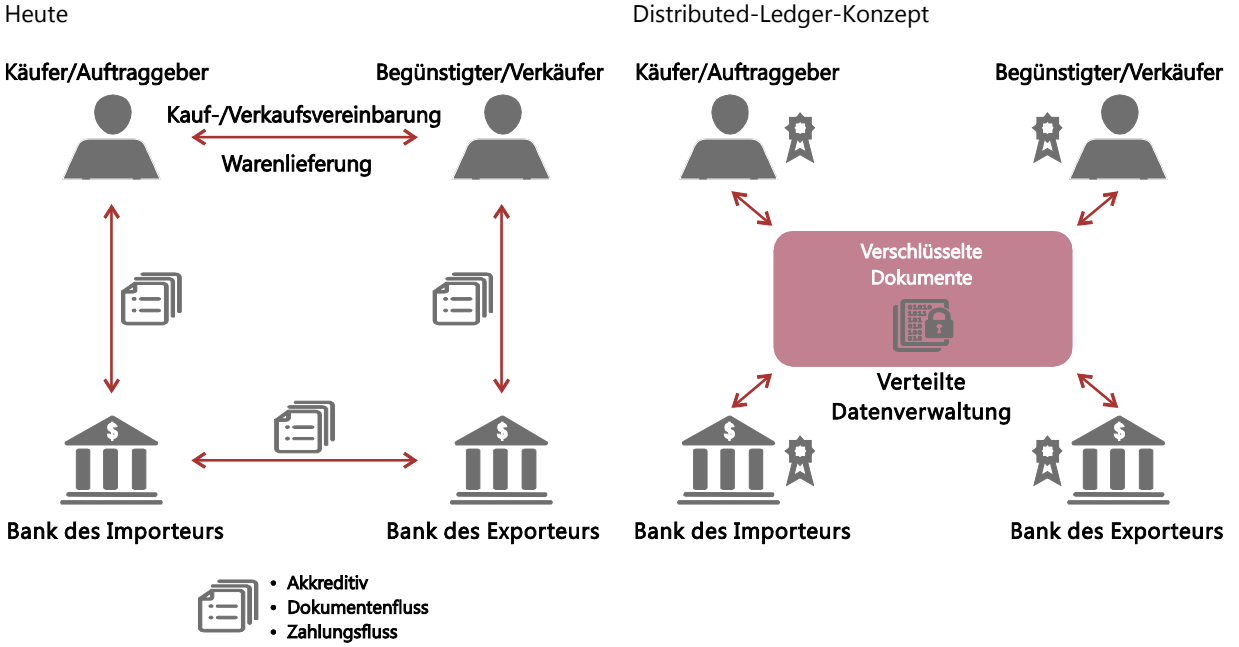
Schätzungen der Welthandelsorganisation zufolge sind 80–90% des Welthandels von Handelsfinanzierungen abhängig. Wenn ein Exporteur und ein Importeur eine Handelsvereinbarung treffen, besteht der Exporteur häufig auf Vorkasse, um nicht das Risiko eingehen zu müssen, nach Lieferung keine Zahlung vom Importeur zu erhalten. Im Gegenzug ist der Importeur darauf bedacht, sein eigenes Risiko zu senken, und verlangt vor Anweisung der Zahlung entsprechende Nachweise über die Lieferung der Ware.

Mit ihren Handelsfinanzierungslösungen schließen Banken und andere Finanzinstitute diese Lücke. In der Regel garantiert eine Bank im Herkunftsland des Importeurs dem Exporteur die Zahlung in Form eines Akkreditivs gegen Vorlage eines Liefernachweises, zum Beispiel eine Verladerechnung. Damit die Transaktion zustande kommt, kann umgekehrt der Exporteur auf Basis dieses Akkreditivs ein Bankdarlehen aufnehmen, wobei der Inkassoerlös von der Bank des Importeurs an die Bank des Exporteurs zu überweisen ist.

Handelsfinanzierungen in ihrer aktuellen Form (Grafik V.B links) sind umständlich, komplex und kostenintensiv. Sie sind verbunden mit einem umfassenden Dokumentenverkehr zwischen dem Exporteur, dem Importeur, den jeweiligen Banken und den Stellen, die die zu liefernde Ware an jedem Kontrollpunkt inspizieren. Weitere involvierte Akteure sind Zollbehörden, Exportversicherungsagenturen bzw. Frachtversicherer. Die diesbezüglichen Dokumente werden oft in Papierform verarbeitet. Mithilfe der Distributed-Ledger-Technologie kann die Ausübung der zugrundeliegenden Verträge vereinfacht werden (Grafik V.B rechts). Beispielsweise könnten mit dem Einsatz von intelligenten Verträgen automatisiert Zahlungen an den Exporteur ausgelöst werden, sobald im System eine gültige Verladerechnung erfasst ist. Außerdem könnte die bessere Verfügbarkeit von Informationen darüber, welche Lieferungen bereits finanziert wurden, das Risiko von Rechtsmissbräuchen schmälern und verhindern, dass Exporteure für dieselbe Lieferung Kredite mehrfach von verschiedenen Banken erhalten.

Handelsfinanzierung unter Nutzung der Distributed-Ledger-Technologie

Grafik V.B



Quelle: Nach www.virtusapolaris.com.

Kasten V.C

Sollten Zentralbanken Digitalgeld ausgeben?

Seit ein paar Jahrzehnten nutzen Zentralbanken aktiv digitale Technologien, um die Effizienz und Solidität des Zahlungsverkehrs und damit des Finanzsystems insgesamt zu verbessern. Dank der digitalen Technologie konnten die Zentralbanken die Liquiditätsbereitstellung für Echtzeit-Bruttoabwicklungssysteme (RTGS) gering halten. Durch die Verknüpfung dieser Systeme mittels Continuous Linked Settlement (CLS) wickeln Geschäftsbanken weltweit täglich Devisengeschäfte rund um die Uhr im Umfang von Billionen von Dollar ab. CLS trägt dazu bei, das Herstatt-Risiko zu eliminieren, d.h. das Risiko, dass eine an einem Devisengeschäft beteiligte Korrespondenzbank in finanzielle Schwierigkeiten gerät, bevor sie die entsprechende Zahlung an den vorgesehenen Empfänger leistet. Dieses Risiko galt zuvor als große Gefahr für die Finanzstabilität. In letzter Zeit ist weltweit ein verstärktes Angebot schnellerer Systeme für den Massenzahlungsverkehr zu beobachten – ein Trend, der von den Zentralbanken aktiv unterstützt und gefördert wird.

Im Rahmen ihrer allgemeinen Vorstöße in den Bereich neuer Zahlungsverkehrstechnologien befassen sich Zentralbanken auch mit der Möglichkeit von digitalem Zentralbankgeld für den Interbankmarkt. Dabei handelt es sich um wertbasierte Versionen herkömmlicher Reserve- und Abwicklungskonten. Entscheidend für den Durchbruch von digitalem Zentralbankgeld für den Interbankmarkt auf Basis der Distributed-Ledger-Technologie ist die Frage, in welchem Umfang diese Technologien die Effizienz steigern und Abwicklungs- und Betriebskosten senken können. Die Einsparungen könnten insofern nennenswert sein, als derzeit viele von Zentralbanken betriebene Massenzahlungssysteme auf veralteten Technologien basieren, die aufwendig gewartet werden müssen.

Die Einführung von digitalem Zentralbankgeld für den Interbankmarkt ist mit zwei wesentlichen Herausforderungen verbunden. Erstens kommt auch bei digitalem Zentralbankgeld für den Interbankmarkt nur ein Distributed-Ledger-Konzept auf Berechtigungsbasis infrage. Zweitens müssen die Optionen für die Konvertierbarkeit von herkömmlichem Zentralbankgeld in digitales Zentralbankgeld und vice versa umsichtig gestaltet werden, um die Innertagsliquidität aufrechtzuerhalten und gleichzeitig das Abwicklungsrisiko zu minimieren.

Eine Reihe von Zentralbanken, darunter die Bank of Canada (Projekt Jasper), die Europäische Zentralbank, die Bank of Japan (Projekt Stella) und die Monetary Authority of Singapore (Projekt Ubin), experimentieren bereits mit dem Betrieb von RTGS-Systemen für den Interbankmarkt, bei denen digitales Zentralbankgeld auf Basis der Distributed-Ledger-Technologie eingesetzt wird. In den meisten Fällen haben sich die Zentralbanken für einen Ansatz mit digitalen Depotscheinen (Digital Depository Receipt, DDR) entschieden. Dabei werden die von der Zentralbank geschöpften digitalen Werte (Token) in „verteilten Konten" gespeichert, wobei der diesbezügliche Deckungsstock in Form von Zentralbankgeld auf einem separaten Konto gehalten wird und gegen diesen einlösbar ist. Die Werte können dann für Interbanktransfers innerhalb des Distributed-Ledger-Systems verwendet werden.

Die Ergebnisse der Experimente werden jetzt nach und nach von den Zentralbanken veröffentlicht. Bei der Nachbildung bestehender Großbetragszahlungssysteme verliefen die einzelnen Experimente in ihrer Anfangsphase größtenteils erfolgreich. Allerdings sind die Resultate nicht eindeutig besser als die mit der bestehenden Infrastruktur zu erzielenden Ergebnisse.①

① Siehe M. Bech und R. Garratt (2017), „Kryptowährungen von Zentralbanken", *BIZ-Quartalsbericht*, September, sowie Ausschuss für Zahlungsverkehr und Marktinfrastrukturen und Märkteausschuss (2018), *Central bank digital currencies,* März.

Fußnoten

[1] Die Terminologie zu diesem Thema ist noch nicht gefestigt, weshalb auch die rechtliche und regulatorische Situation nicht eindeutig ist. Die hier verwendete Bezeichnung „Kryptowährungen" ist nicht als Ausdruck einer bestimmten Meinung zur Systemgrundlage zu verstehen; Systeme auf Protokollbasis haben üblicherweise bestimmte, aber nicht alle Charakteristika einer offiziellen Währung und werden je nach geltendem nationalen Recht unterschiedlich behandelt. Auf einzelne Kryptowährungen bzw. Kryptoanlagen wird nachfolgend beispielhaft Bezug genommen. Dabei handelt es sich aber weder um umfassende Darstellungen noch um eine Parteinahme seitens der BIZ oder ihrer Aktionäre für bestimmte Kryptowährungen, Firmen, Produkte oder Leistungen.

[2] Siehe dazu auch Carstens (2018a,c).

[3] Graeber (2011) argumentiert, dass sich das Geldwesen erst mit dem Auftauchen von Münzen ausbreitete; die ersten Münzen tauchten um 600 bis 500 vor Christus nahezu zeitgleich in China, Indien und Lydien (der heutigen Türkei) auf. Entgegen der weit verbreiteten Annahme wechselten Güter vor der Entstehung des Geldes hauptsächlich auf Basis bilateraler Schuldscheine und nicht im Tauschhandel die Hände.

[4] Zu den Funktionen von Geld gibt es umfassende Darstellungen in der Fachliteratur; u.a. zeigen Kiyotaki und Wright (1989), dass der Tauschhandel durch das Tauschmittel Geld optimiert werden kann. Kocherlakota (1996) zeigt, dass sich die „Gedächtnisfunktion" des Geldes positiv auf das Ergebnis auswirkt, wenn die Transaktionen unüberschaubar werden und nicht gesichert sind. Samuelson (1958) veranschaulicht in einem überlappenden Generationenmodell, dass Geld als Wertaufbewahrungsmittel effizienzsteigernd wirken kann. Doepke und Schneider (2017) zeigen, wie eine gemeinsame Recheneinheit zu besseren Ergebnissen führt und wieso staatliches Geld Recheneinheit und Tauschmittel zugleich ist.

[5] Als Warengeld fungierten etwa Muscheln in Afrika, Kakaobohnen bei den Azteken und Muschelgürtel (Wampum) in nordamerikanischen Kolonien. Dabei dürften sogar in diesen Fällen parallel zum Warengeld Kreditbeziehungen existiert haben. Eine detailliertere Darstellung findet sich u.a. bei Melitz (1974).

[6] Zur Geschichte der Akkreditive und ihrer zentralen Rolle bei der Entwicklung des Geldwesens im Allgemeinen und bei der Handelsfinanzierung im Besonderen siehe De Roover (1948, 1953). Ein geschichtlicher Überblick samt detaillierter Analyse findet sich bei Kindleberger (1984) und, mit Fokus auf die wichtige Einführung der solidarischen Haftung, bei Santarosa (2015).

[7] Aus diesem Spannungsfeld heraus lassen sich u.a. auch Versuche erklären, als Deckungsstock für das staatliche Geld auf Rohstoffe (wie beim sog. Goldstandard) zurückzugreifen. Ein derartiges System sorgt normalerweise für Stabilität, engt aber den Spielraum der Zentralbank in finanziell und wirtschaftlich schwierigen Zeiten bei der Anpassung der Geldmenge ein. Im Extremfall wurde dieses Problem oft mit dem Aussetzen der Konvertibilität umgangen. So sollte beim Goldstandard die Goldkonvertibilität den Souverän an der übermäßigen Geldausgabe hindern und somit Geldentwertung auf diesem Weg verhindern. Dieses Konstrukt war glaubwürdig, weil der Rohstoff über die geldpolitische Rolle als Zahlungsmittel hinaus einen Marktwert hat. Dies hinderte den Souverän daran, kraft seiner Monopolstellung die Goldanleger quasi in Geiselhaft zu nehmen. Dies wird in Giannini (2011) näher ausgeführt.

[8] Eine aktuelle Darstellung samt einer Analyse der Anreize zur Geldentwertung findet sich bei Schnabel und Shin (2018).

[9] Siehe Van Dillen (1964), Roberds und Velde (2014) sowie Bindseil (2018). Auf den Konnex zum Zentralbankwesen gehen Ugolini (2017), Bindseil (2018) sowie Schnabel und Shin (2018) ein.

[10] Außerdem können Zentralbanken in der Regel mit der nötigen Flexibilität reagieren, um in letzter Instanz als Kreditgeber einzuspringen. Die Große Finanzkrise hat einmal mehr vor Augen geführt, wie fragil – aber auch wie flexibel – die derzeitigen geldpolitischen Systeme selbst in den am meisten fortgeschrittenen Volkswirtschaften sind. Während die Krise die regulatorischen Unzulänglichkeiten zutage brachte, hat das verstärkte Augenmerk auf die Bankenaufsicht und -regulierung nach der Krise gezeigt, wie das institutionelle Fundament verbessert werden kann, um das Vertrauen in Geld angesichts der zweistufigen Geldschöpfung (durch die Zentralbanken und die Geschäftsbanken) aufrechtzuerhalten.

[11] Siehe Carstens (2018a). Giannini (2011) unterstreicht die Bedeutung des institutionellen Fundaments der Geldversorgung ebenfalls: „Die Entwicklung der monetären Institute ist offenbar vor allem Ausdruck des fortwährenden Dialogs zwischen der Wirtschaft und der Politik, wobei beide Seiten abwechselnd für monetäre Innovationen sorgen (…) und die gemeinsamen Interessen vor dem Missbrauch durch Partikularinteressen schützen."

[12] So überwachen Zentralbanken heute den Zahlungsverkehr und stellen hohe Beträge an Innertageskrediten zur Verfügung, um vor allem im Großbetragszahlungsverkehr die Geldversorgung zu sichern. Je nach Ausgestaltung der Systeme können die Kredite auch bis zum nächsten Geschäftstag oder für längere Laufzeiten zur Verfügung gestellt werden. Eine weiterführende Erläuterung der Systeme und operativen Verfahren sowie sonstiger Themen findet sich in BIZ (1994) und Borio (1997).

[13] Eine detaillierte Darstellung findet sich in Bech und Garratt (2017) sowie in CPMI-MC (2018).

[14] Wie bei Banknoten und anderen physischen Werten wird jede Transaktion unter Bezugnahme auf das Zahlungsmittel, nämlich den jeweiligen Ledger-Eintrag, validiert. Damit unterscheidet sich dieses System von anderen Formen elektronischen Geldes, bei denen die Validierung auf der Identität des Kontoinhabers basiert. Bei den Kryptowährungen handelt es sich also um wertbasiertes Digitalgeld (Token).

[15] Beispiele für aktuelle oder geplante Kryptowährungen auf Berechtigungsbasis und mit designierten Trusted Nodes sind etwa die sog. Utility Settlement Coin und das geplante Digitalgeldprojekt „Ripple" der SAGA-Stiftung.

[16] „Bitcoin" steht in diesem Bericht je nach Kontext sowohl für das Protokoll und das gesamte Teilnehmernetzwerk als auch für die Werteinheit.

[17] Beispiele sind etwa Ethereum, Litecoin und Namecoin.

[18] Auer (2018) beschreibt die technischen Elemente von Bitcoin und anderen auf dem Blockchain-Konzept basierenden Kryptowährungen, wie digitale Signaturen, Hashfunktionen und die kryptografische Verkettung von Blöcken. Siehe auch Berentsen und Schär (2018).

[19] Technisch erfolgt die Umsetzung mittels eines kryptografischen Hash-Algorithmus – beispielsweise SHA-256 im Fall von Bitcoin. Typisch für diese Hash-Algorithmen sind, dass ein bestimmter Wert nur nach dem Trial-und-Error-Prinzip generiert werden kann.

[20] Damit eine Kryptowährung ohne Berechtigungssystem in einem Umfeld funktioniert, das gänzlich ohne vertrauensbildende Instanz auskommt, muss jeder Miner und Nutzer immer eine Kopie der gesamten aktuellen Transaktionshistorie abspeichern. Allerdings verlassen sich viele Nutzer in der Praxis auf die Angaben anderer. Einzelne Nutzer beschränken sich darauf, in einem vereinfachten Validierungsprozess nur summarische Angaben zu validieren. Hinzu kommt, dass eine noch größere Zahl von Nutzern im Gegensatz zur ursprünglichen Idee hinter Bitcoin nur über die Website Dritter auf ihre Mittel zugreifen können. In diesen Fällen kann nur diese Drittpartei über die Kryptowährungsguthaben ihrer Klienten verfügen.

[21] Nakamoto (2009), S. 8.

[22] Dies ergibt sich aus der Selbstkalibrierung des Leistungsnachweises, wonach das erforderliche mathematische Schwierigkeitsniveau so lange steigt, bis die gemeinsame Rechenleistung aller Miner gerade noch ausreicht, um die Transaktionshistorie zu dem laut Protokoll vorgegebenen Tempo zu aktualisieren.

[23] Siehe Carstens (2018a).

[24] Während das Stauproblem mit einer Anhebung der Blockgröße in den Griff zu bekommen wäre, könnte dies in Wirklichkeit kontraproduktiv sein. Abgesehen von der Miner-Vergütung muss ein gewisser Stau entstehen, damit die Nutzer angehalten sind, für ihre Transaktionen zu zahlen. Wenn das System alle Transaktionen bearbeitet, bieten rational agierende Nutzer eine Transaktionsgebühr von marginal über null. Damit ginge der Nutzen der Miner aus der Fortschreibung der Transaktionshistorie gegen null, wodurch das Gleichgewicht zusammenbrechen könnte. Siehe insbesondere Hubermann et al. (2017), Easley et al. (2017) sowie Abadi und Brunnermeier (2018).

[25] Technisch betrachtet interagieren die Nutzer nicht strategisch komplementär, sondern als strategische Substitute. Spieltheoretisch betrachtet sind Kryptowährungen daher ein Stauspiel, kein Koordinationsspiel.

[26] Die probabilistische Natur der Finalität könnte insbesondere Aggregationsrisiken erzeugen, wenn im Großkundensegment, wo Gelder in der Regel sofort neu angelegt werden, mit Kryptowährungen bezahlt würde. Damit würde eine komplett neue Dimension des Aggregationsrisikos entstehen, weil Forderungen über die Wahrscheinlichkeit der Nichtfinalität der gesamten Transaktionshistorie aneinander gekoppelt wären.

[27] An Lösungsvorschlägen mangelt es nicht, aber die meisten Vorschläge müssen erst noch den Praxistest bestehen. Beispielsweise könnten Kryptowährungsprotokolle künftig so konzipiert sein, dass der kostspielige Leistungsnachweis (Proof of Work) durch einen Anteilsnachweis (Proof of Stake)

abgelöst wird. Unter den Lösungsvorschlägen für das Skalierungsproblem findet sich das Lightning Network, das kleine Transaktionen im Wesentlichen von der Haupt-Blockchain auf ein separates System auf Wertkartenbasis umlenkt. Schließlich gibt es auch neue Kryptowährungen wie IOTA, die die Blockchain durch eine komplexere Ledger- und Validierungsstruktur ersetzen wollen.

[28] Siehe Juskalian (2018).

[29] Siehe Carstens (2018a,b).

[30] Selbst Beamte sind nicht immun gegen die Verlockungen von Kryptowährungen: Zwei US-Regierungsmitarbeiter wurden des Bitcoin-Diebstahls im Zusammenhang mit Konfiszierungen bei der Silk-Road-Schließung angeklagt.

[31] So werden wohl die meisten per Smartphone gemachten Bitcoin-Zahlungen mit ziemlicher Sicherheit über Dritte abgewickelt, weil die Blockchain schon so groß geworden ist, dass die Speicherkapazität der meisten Smartphones dafür nicht mehr ausreicht. Reuters (2017) sowie Moore und Christin (2013) nennen eine Reihe von Vorfällen mit Drittparteien, die sich entweder als kriminell erwiesen oder gehackt wurden. Für eine Analyse der illegalen Nutzung von Kryptowährungen siehe Fanusie und Robinson (2018) sowie Foley et al. (2018).

[32] Siehe G20 Finance Ministers and Central Bank Governors (2018).

[33] Clayton (2017) diskutiert die Regulierung von ICOs in Gegenüberstellung zu IPOs aus Sicht der USA und stellt diesbezüglich fest: „Wenn es sich auch um unterschiedliche Wertpapierkonzepte handelt, so ändert sich nichts an der fundamentalen Tatsache, dass die Wertpapiervorschriften eingehalten werden müssen, wenn ein Wertpapier begeben wird." FINMA (2018) definiert den regulatorischen Rahmen für ICOs in der Schweiz und unterscheidet in der Klassifizierung nach der effektiven Nutzung der Werte (Token): im Zahlungsverkehr, als Geldanlage oder für andere Zwecke (Utility Token).

[34] Faktisch ist der Betrieb protokollbasierter Kryptowährungen mit der Zulassung in einem einzigen Land möglich. Dass es den Aufsichtsinstanzen Schwierigkeiten bereitet, illegale Downloadseiten wie Napster oder Pirate Bay und Downloadprotokolle wie BitTorrent zu sperren, zeigt, an welche Grenzen die Durchsetzbarkeit stößt.

[35] In Financial Action Task Force (2015) wird argumentiert, dass es wichtig ist, ähnliche Produkte und Dienstleistungen in allen Ländern je nach Funktion und Risikoprofil konsistent zu behandeln, um die Wirksamkeit der internationalen Standards zur Bekämpfung von Geldwäsche zu stärken.

[36] Eine Komplikation besteht darin, dass die Zahlungen von diversen Instanzen – wie der Zahlungsverkehrsaufsicht, der Finanzaufsicht, der Konsumentenschutzbehörde und den Stellen zur Bekämpfung von Terrorismusfinanzierung und Geldwäsche – und durch Gesetze mit sehr unterschiedlichen Zielsetzungen reguliert werden. So gelten für in den USA ansässige Institute eine ganze Reihe von Gesetzen und Bestimmungen (Bank Secrecy Act, USA PATRIOT Act, Office of Foreign Assets Control Regulations etc.). Weitere Komplikationen ergeben sich aus der Anwendbarkeit bestehender Gesetzesbestimmungen auf neue Instrumente. So ist elektronisches Geld laut EU-Recht so definiert, dass die Guthaben eine Forderung gegenüber der ausgebenden Stelle darstellen müssen. Da Kryptowährungen aber keine Forderungen darstellen, fallen sie nicht unter die Definition von elektronischem Geld und dementsprechend auch nicht unter die jeweiligen Rechtsbestimmungen.

[37] Technisch ließe sich wertbasiertes (token-based) digitales Zentralbankgeld auf vielfache Weise umsetzen. Dabei ist die Anwendung der Distributed-Ledger-Technologie analog zum Modell der Kryptowährungen denkbar, aber mit dem Unterschied, dass die Geldmenge von der Zentralbank bestimmt wird und nicht im Protokoll festgelegt ist, und dass die Zentralbank den Token-Kurs garantiert.

[38] CPMI-MC (2018).

Bibliografie

Abadi, J. und M. Brunnermeier (2018): „Blockchain economics", Princeton University, Mimeo, Mai.

Auer, R. (2018): „The mechanics of decentralised trust in Bitcoin and the blockchain", *BIS Working Papers*, erscheint demnächst.

Ausschuss für Zahlungsverkehr und Marktinfrastrukturen und Märkteausschuss (CPMI-MC 2017): *Central bank digital currencies*, März.

Bank für Internationalen Zahlungsausgleich (1994): *64. Jahresbericht*, Juni.

Bech, M. und R. Garratt (2017): „Kryptowährungen von Zentralbanken", *BIZ-Quartalsbericht*, September.

Berentsen, A. und F. Schär (2018): „A short introduction to the world of cryptocurrencies", Federal Reserve Bank of St Louis, *Review*, Vol. 100, Nr. 1.

Bindseil, U. (2018): „Pre-1800 central bank operations and the origins of central banking", Universität Mannheim, Mimeo.

Borio, C. (1997): „The implementation of monetary policy in industrial countries: a survey", *BIS Economic Papers,* Nr. 47, Juli.

Carstens, A. (2018a): „Money in the digital age: what role for central banks?", Vortrag im House of Finance der Goethe-Universität, Frankfurt, 6. Februar.

——— (2018b): „Central banks and cryptocurrencies: guarding trust in a digital age", Vortrag in der Brookings Institution, Washington DC, 17. April.

——— (2018c): „Technologie kann Vertrauen nicht ersetzen", *Börsen-Zeitung*, 23. Mai.

Catalini, C., J. Boslego und K. Zhang (2018): „Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", *MIT Working Papers*, erscheint demnächst.

Clayton, J. (2017): „Statement on cryptocurrencies and initial coin offerings", www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 11. Dezember.

De Roover, R. (1948): *Money, banking and credit in mediaeval Bruges: Italian merchant-bankers Lombards and money changers – a study in the origins of banking,* Mediaeval Academy of America.

——— (1953): *L'évolution de la lettre de change: XIVe-XVIIIe siècle*, Armand Colin.

Doepke, M. und M. Schneider (2017): „Money as a unit of account", *Econometrica*, Vol. 85, Nr. 5, S. 1537–1574.

Easley, D., M. O'Hara und S. Basu (2017): „From mining to markets: The evolution of Bitcoin transaction fees", papers.ssrn.com/sol3/papers.cfm?abstract_id=3055380.

Eidgenössische Finanzmarktaufsicht (FINMA 2018): *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16. Februar.

Fanusie, Y. und T. Robinson (2018): „Bitcoin laundering: an analysis of illicit flows into digital currency services", Center on Sanctions & Illicit Finance Memorandum, Januar.

Financial Action Task Force (2015): *Guidance for a risk-based approach to virtual currencies*, Juni.

Foley, S., J. Karlsen und T. Putniņš (2018): „Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", dx.doi.org/10.2139/ssrn.3102645.

G20 Finance Ministers and Central Bank Governors (2018): Kommuniqué zum Gipfeltreffen in Buenos Aires, 19./20. März.

Giannini, C. (2011): *The age of central banks*, Edward Elgar.

Graeber, D. (2011): *Debt: the first 5,000 years*, Melville House.

Huberman, G., J. Leshno und C. Moellemi (2017): „Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", *Columbia Business School Research Papers*, Nr. 17–92.

Juskalian, R. (2018): „Inside the Jordan refugee camp that runs on blockchain", *MIT Technology Review*, Online-Ausgabe, 12. April.

Kindleberger, C. (1984): *A financial history of western Europe*, Allen & Unwin.

Kiyotaki, N. und R. Wright (1989): „On money as a medium of exchange", *Journal of Political Economy*, Vol. 97, Nr. 4, S. 927–954.

Kocherlakota, N. (1996): „Money is memory", *Journal of Economic Theory*, Vol. 81, Nr. 2, S. 232–251.

Melitz, J. (1974): *Primitive and modern money: an interdisciplinary approach*, Addison-Wesley.

Moore, T. und N. Christin (2013): „Beware the middleman: empirical analysis of Bitcoin-exchange risk", in: A.-R. Sadeghi (Hrsg.), *Lecture Notes in Computer Science*, Vol. 7859.

Nakamoto, S. (2009): „Bitcoin: a peer-to-peer electronic cash system", Weißbuch.

Reuters (2017): „Cryptocurrency exchanges are increasingly roiled by hackings and chaos", 29. September.

Roberds, W. und F. Velde (2014): „Early public banks", *Federal Reserve Bank of Chicago Working Papers*, Nr. 2014–03.

Samuelson, P. (1958): „An exact consumption-loan model of interest with or without the social contrivance of money", *Journal of Political Economy*, Vol. 66, Nr. 6, S. 467–482.

Santarosa, V. (2015): „Financing long-distance trade: the joint liability rule and bills of exchange in eighteenth-century France", *The Journal of Economic History*, Vol. 75, Nr. 3, S. 690–719.

Schnabel, I. und H. S. Shin (2018): „Money and trust: lessons from the 1620s for money in the digital age", *BIS Working Papers*, Nr. 698, Februar.

Ugolini, S. (2017): *The evolution of central banking: theory and history*, Palgrave-Macmillan.

Van Dillen, J. G. (1964): *History of the principal public banks*, Frank Cass & Co.