



**No. 15-2017**

**Andreas Hanl und Jochen Michaelis**

## **Kryptowährungen- Ein Problem für die Geldpolitik?**

This paper can be downloaded from  
<http://www.uni-marburg.de/fb02/makro/forschung/magkspapers>

Coordination: Bernd Hayo • Philipps-University Marburg  
School of Business and Economics • Universitätsstraße 24, D-35032 Marburg  
Tel: +49-6421-2823091, Fax: +49-6421-2823088, e-mail: [hayo@wiwi.uni-marburg.de](mailto:hayo@wiwi.uni-marburg.de)

# **Kryptowährungen – Ein Problem für die Geldpolitik?**

**Andreas Hanl<sup>\*</sup> und Jochen Michaelis<sup>\*\*</sup>**

**10. März 2017**

## *Abstract*

Cryptocurrencies such as Bitcoins may revolutionize the financial system by at least partially replacing intermediaries such as central banks and commercial banks. The blockchain technology enables users to transact on a peer-to-peer basis. This imposes a serious threat on the financial intermediaries as well as on monetary policy authorities. In this paper, we examine how well cryptocurrencies fulfill the functions of a fiat money and discuss the comparative advantages of cryptocurrencies. We proceed by exploring the implications of digital currencies for the concept and conduct of monetary policy.

*JEL Classification:* E42, E52

*Key words:* Bitcoin, Kryptowährung, Geldpolitik

Andreas Hanl  
Institut für Volkswirtschaftslehre  
Nora-Platiel-Str. 4  
34109 Kassel  
Tel.: 0561-804 3887  
  
Email: hanl(at)uni-kassel.de

Prof. Dr. Jochen Michaelis  
Institut für Volkswirtschaftslehre  
Nora-Platiel-Str. 4  
34109 Kassel  
Tel.: 0561-804 3562  
Fax: 0561-804 3083  
  
Email: michaelis(at)wirtschaft.uni-kassel.de

---

\* Andreas Hanl, M.Sc. ist Doktorand am Lehrstuhl für Geld, Kredit und Währung an der Universität Kassel.

\*\* Prof. Dr. Jochen Michaelis ist Inhaber des Lehrstuhls für Geld, Kredit, Währung an der Universität Kassel.

Einen Vermögensgegenstand, der die Tauschmittelfunktion erfüllt, bezeichnet man als Geld. Die Erscheinungsformen des Geldes haben sich im Laufe der Zeit gewandelt, vom Warengeld über Münzen und Papiergeld zu stoffwertlosem Giralgeld. Die jüngste Entwicklung sind Kryptowährungen (KW) wie das von Satoshi Nakamoto konzipierte und mit der Bezeichnung „Bitcoin“ versehene System.<sup>1</sup> Insbesondere zwei Eigenschaften sind kennzeichnend für KW: Weil sie die Blockchain-Technologie nutzen, kann bei Geldgeschäften aller Art auf die Einschaltung eines vertrauenswürdigen Dritten verzichtet werden. Bei Finanzgeschäften sind dies in der Regel die Geschäftsbanken, bei grenzüberschreitenden Geldtransfers die Zentralbanken.<sup>2</sup> Zudem erodiert das staatliche Notenmonopol. Bis dato werden KW ausschließlich von Privaten emittiert, es gibt hierbei keine Abhängigkeiten von staatlichen Institutionen. Damit fällt auch der reale Ertrag aus der Geldemission (Seigniorage) ausschließlich den Privaten zu.

Die Zentralbanken sind sich der Herausforderungen bewusst, entsprechend haben sie die KW auf ihre Forschungsagenda gesetzt.<sup>3</sup> Die Problemfelder sind vielfältig: Kann die Stabilität der Zahlungs- und Verrechnungssysteme weiterhin gewährleistet werden? Welche Faktoren bestimmen die Nachfrage nach KW und inwieweit substituiert dies die Nachfrage nach herkömmlichen Zentralbankgeld? Welche Rückwirkungen auf die Wirkungsweise und die Ausgestaltung der Geldpolitik sind zu erwarten? Können Zentralbanken der Erosion des Notenmonopols entgegenwirken durch Ausgabe eigener Kryptowährungen? Ziel dieses Beitrags ist, einzelne Aspekte dieser Diskussion zu vertiefen.

### **Sind Kryptowährungen Geld?**

Ökonomen definieren Geld als alles, was *allgemein* zur Bezahlung von Gütern und Dienstleistungen sowie zur Begleichung von Schulden akzeptiert wird. Die Konkretisierung dieser Definition erfolgt meist mit Hilfe der drei Geldfunktionen (Tauschmittel, Recheneinheit, Wertaufbewahrung). Wie die nachfolgende Diskussion zeigen wird, ist insbesondere das Kriterium der generellen Akzeptanz (noch) nicht erfüllt, sodass KW von den Zentralbanken aber auch in der einschlägigen Fachliteratur die Geldeigenschaft abgesprochen

---

<sup>1</sup> S. Nakamoto: Bitcoin – A Peer-to-Peer Electronic Cash System, 2008. <https://bitcoin.org/bitcoin.pdf>.

<sup>2</sup> Allgemeinverständliche Beschreibungen der Blockchain-Technologie sowie des Bitcoin-Systems finden sich bei V. Brühl: Bitcoins, Blockchain und Distributed Ledgers: Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, in: Wirtschaftsdienst, 97. Jg. (2017), H. 2, S. 135 – 142; W. Blocher: The Next Big Thing: Blockchain – Bitcoin – Smart Contracts: Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird, in: Anwaltsblatt, 66. Jg. (2016), H. 8+9, S. 612 – 618.

<sup>3</sup> Vgl. z.B. Europäische Zentralbank: Virtual Currency Schemes – A Further Analysis, Frankfurt a.M. 2015; R. Ali, J. Barrdear, R. Clews und J. Southgate: Innovations in Payment Technologies and the Emergence of Digital Currencies, in: Bank of England Quarterly Bulletin, Q3/2014, S. 262 – 275.

wird.<sup>4</sup> Allerdings ist allen Beteiligten bewusst, dass dieses Verdikt eine Momentaufnahme ist, nicht zuletzt die extrem dynamische technologische Entwicklung kann sehr schnell eine Neubewertung erforderlich machen.

Ähnlich wie Papiergeld oder Giralgeld haben KW keinen intrinsischen Wert. Ein Nutzer wird KW nur dann als Tauschmittel akzeptieren, wenn er darauf vertrauen kann, dass zu einem zukünftigen Zeitpunkt eine hinreichend große Zahl von anderen Akteuren bereit sein wird, die KW wieder gegen Güter und Dienstleistungen einzutauschen. Diese Vertrauensabhängigkeit ist allen Währungen immanent, insbesondere gilt sie im selben Maße für ein gesetzliches Zahlungsmittel. Durch die Festlegung eines gesetzlichen Zahlungsmittels kann der Staat zwar versuchen, ein solches Vertrauen zu generieren, aber die Eigenschaft des gesetzlichen Zahlungsmittels ist weder notwendig noch hinreichend für die Tauschmittelfunktion. Sowohl gesetzliche Zahlungsmittel als auch KW sind sog. Außengeld, d.h. dem Vermögen gemessen in Euro oder in Bitcoins steht keine gleichhohe Verbindlichkeit eines anderen Akteurs gegenüber. Beim Euro oder beim US-Dollar ist eine Banknote juristisch zwar eine Forderung gegenüber der Zentralbank, mithin für die Zentralbank eine Verbindlichkeit. Aber da die Verbindlichkeit keine Verpflichtung zum Umtausch der Banknote in Güter oder Dienstleistungen beinhaltet, steht sie im wahrsten Sinne des Wortes nur auf dem Papier. Um als Tauschmittel zu dienen, müssen gesetzliche Zahlungsmittel wie auch KW gleichermaßen besagtes Vertrauen gewinnen bspw. durch das Erzeugen von Wertstabilität.

Die Zahl und das Volumen der in KW abgewickelten Geschäfte sind bis dato vergleichsweise gering. Derzeit (Stand März 2017) werden weltweit etwa 300.000 Transaktionen pro Tag mit Hilfe des Bitcoin-Netzwerks getätigt, die technische Kapazität von ca. sieben Transaktionen pro Sekunde ist damit zur Hälfte ausgeschöpft. Im Vergleich dazu werden allein in Deutschland werktäglich ca. 25 Millionen Überweisungen getätigt, und etablierte Online-Bezahlverfahren wie Visa oder Mastercard leisten bis zu 2.000 Transaktionen pro Sekunde.<sup>5</sup> Bei den KW sind die technologischen Restriktionen noch gravierend, aber von der ersten Generation einer neuen Technologie sollte man nicht mehr erwarten als die grundsätzliche Funktionsfähigkeit des Systems, und die ist zweifelsohne gegeben.

---

<sup>4</sup> Vgl. D. Yermack: Is Bitcoin a Real Currency? An Economic Appraisal, in D. K. C. Lee (Hrsg.): Handbook of Digital Currency, Amsterdam, 2015, S. 31 – 43; S. Lo und C Wang, Bitcoin as Money?, in: Current Policy Perspectives, No. 14-4, 2014, Federal Reserve Bank of Boston.

<sup>5</sup> Vgl. Deutsche Bundesbank: Zahlungsverhalten in Deutschland 2014: Dritte Studie über die Verwendung von Bargeld und unbaren Zahlungsinstrumenten, Frankfurt, 2015; P. Franco: Understanding Bitcoin: Cryptography, Engineering and Economics, Chichester 2015.

Kryptowährungen sind ein Netzwerk-Gut – dies ist für die Etablierung als Tauschmittel ungleich bedeutsamer als die aktuellen technologischen Restriktionen. Warum sollten Kunden auf KW umsteigen, wenn KW nur in wenigen Geschäften akzeptiert werden? Und warum sollten Geschäftsinhaber KW akzeptieren, wenn nur wenige Kunden damit zu zahlen wünschen? Weil der Konsum von Netzwerk-Gütern mit positiven externen Effekten einhergeht, stellt der Markt eine „zu geringe“ Menge zur Verfügung. Selbst wenn alle Beteiligten die grundsätzliche Überlegenheit der neuen Zahlungstechnologie kennen und akzeptieren, können Netzwerkeffekte plus Wechselkosten den Übergang zur neuen Technologie verhindern. Die dezentrale Organisation des Systems erschwert das Erreichen der kritischen Masse an Nutzern, gleichwohl dürfte das Überwinden dieser Schwelle die Nagelprobe sein, die letztlich über den Erfolg von KW entscheidet. Eine Hyperinflation gesetzlicher Währungen oder die Ernennung einer KW zum gesetzlichen Zahlungsmittel würden das Verlassen des inferioren Gleichgewichts erleichtern, aber mit solchen Szenarien ist nicht zu rechnen.<sup>6</sup>

Nun ist die Verwendung einer Zahlungstechnologie in der Regel keine 0-1-Entscheidung. Der typische Konsument nutzt zwei oder drei Methoden, bspw. Bargeld für die täglichen Einkäufe und Kreditkarten für größere Transaktionen. Eine neue Zahlungsmethode wie die KW muss daher nicht für alle Transaktionen nach allen Kriterien wie Kosten, Geschwindigkeit oder Sicherheit den bisherigen Technologien überlegen sein, sondern die Überlegenheit in einzelnen Teilbereichen reicht aus, um eine substantielle Verbreitung zu finden. Wie empirische Studien zeigen, reagieren Konsumenten durchaus sensitiv mit der Wahl der Zahlungsmethode, wenn die neue Technologie ein besseres Matching mit ihren Bedürfnissen erlaubt.<sup>7</sup>

Etwas paradox zumindest beim Bitcoin: Die Verwendung als Tauschmittel ist begrenzt, gerade weil er ein erfolgreiches Wertaufbewahrungsmittel ist. Wie in Abb. 1 veranschaulicht, sind die Wertsteigerungen des Bitcoins im Vergleich zum US-Dollar zumindest seit 2013 exorbitant. Die Wertsteigerungen sind alles andere als stetig, aber eine buy-and-hold-Strategie erscheint lukrativ. Neben dem Interesse an einer neuen Technologie ist die Funktion als Wertanlage das bedeutsamste Motiv für das Halten von Bitcoins. Zumindest für die US-Konsumenten ist dieses Motiv bedeutsamer als die Nachfrage nach Bitcoins zwecks

---

<sup>6</sup> Vgl. hierzu W. Luther: Cryptocurrencies, Network Effects, and Switching Costs, in: Contemporary Economic Policy, 34. Jg. (2016), H. 3, S. 553 – 571.

<sup>7</sup> Vgl. S. Koulayev, M. Rysman, S. Schuh, und J. Stavins, Explaining Adoption and Use of Payment Instruments by US Consumers, in: RAND Journal of Economics, 47. Jg. (2016), H. 2, S. 293 – 325.

Abwicklung von Käufen von Gütern und Dienstleistungen.<sup>8</sup> In eine ähnliche Richtung deutet die Verwendung neu geschürfter Bitcoins, sie werden mehrheitlich nicht verausgabt, sondern bleiben als Vermögensanlage in Händen des Miners.<sup>9</sup>

Die Eigenschaft als Wertaufbewahrungsmittel ist unter Hinweis auf die extreme Volatilität des Bitcoin-Kurses (vgl. Abb. 1) durchaus strittig. Die Tagesschwankungen des Bitcoin-Wechselkurses zum US-Dollar betragen häufig mehrere Prozent, sodass ein intertemporaler Vermögenstransfer von heute nach morgen oder übermorgen mitunter nicht wertstabil erfolgt. Die hohe Volatilität reflektiert den geringen Liquiditätsgrad des Bitcoin-Marktes. Angesichts der derzeit rund 16 Millionen umlaufenden Bitcoins ist das Handelsvolumen gering, und wie bei einem „thin market“ zu erwarten, führen bereits kleinere Änderungen in Angebot und/oder Nachfrage zu substantiellen Kursausschlägen. Weil die Zahl der maximal umlaufenden Bitcoins technologisch fixiert ist, wird auch zukünftig der Bitcoin-Markt wenig liquide sein, die hohe Kursvolatilität wird sich nicht mindern. Für risikoscheue Konsumenten mag dies ein hinreichender Grund sein, gar nicht erst mit KW wie den Bitcoin zu experimentieren. Auf jeden Fall ist dies eine zusätzliche Hürde für die allgemeine Akzeptanz als Zahlungsmittel.

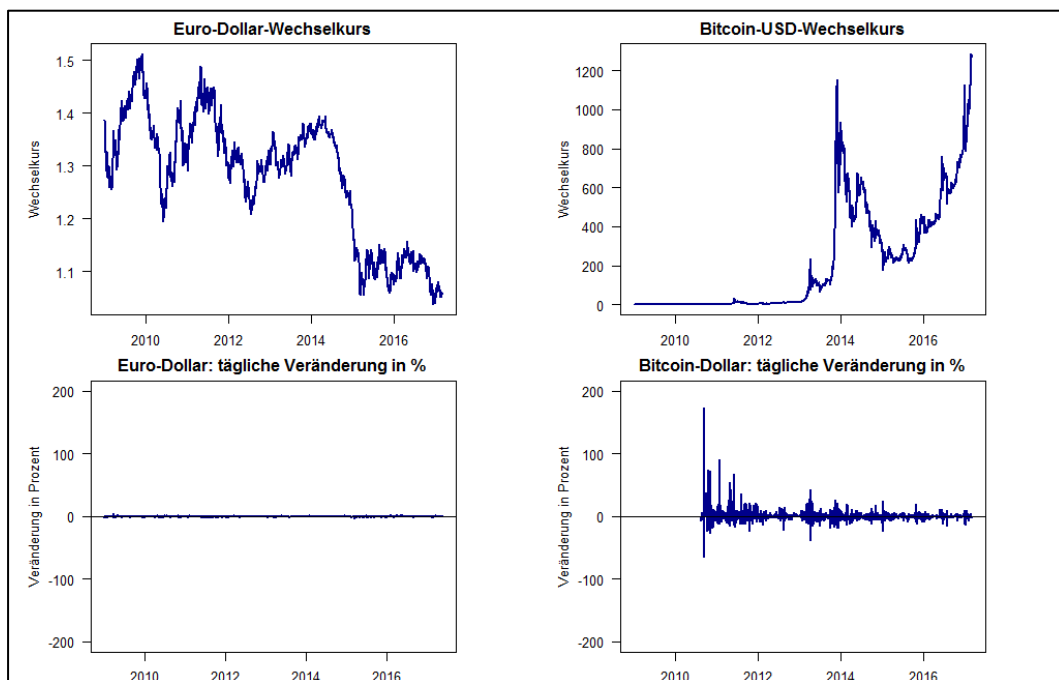


Abbildung 1: Volatilität des Bitcoin-US-Dollar-Wechselkurses im Vergleich zum Euro-Dollar-Wechselkurs. Abbildung basiert auf Daten von Quandl und eigenen Berechnungen.

<sup>8</sup> S. Schuh und O. Shy, U.S. Consumers' Adoption and Use of Bitcoin and other Virtual Currencies, Working Paper 2015, <http://www.banqueducanada.ca/wp-content/uploads/2015/12/us-consumers-adoption.pdf>.

<sup>9</sup> Vgl. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker und S. Savage: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, in: IMC '13 Proceedings of the 2013 conference on Internet measurement conference, S. 127 – 140.

Die hohe Kursvolatilität generiert zwei weitere Effekte. Erstens, Spiegelbild des Wechselkursrisikos ist die Unsicherheit über den Realwert einer Transaktion. Dies gilt für Käufer wie auch Verkäufer einer Ware. Letztere reagieren hierauf häufig mit dem Einsatz eines Dienstleisters (einer Software), die den sofortigen Umtausch von eingenommenen Bitcoins in Euro oder US-Dollar vornimmt und den Gegenwert dem Verkäufer gutschreibt. In diesem Fall zahlen die Konsumenten zwar mit Bitcoin, aber es ist unklar, ob man wirklich sagen kann, dass die Verkäufer Bitcoin akzeptieren.<sup>10</sup> Und zweitens, die hohe Kursvolatilität verhindert die Nutzung des Bitcoins als Recheneinheit. Auch die Unternehmen, die Bitcoin akzeptieren, formulieren ihre Preise in Euro bzw. US-Dollar, der Bitcoin-Preis ergibt sich erst nach Umrechnung mit dem aktuellen Wechselkurs. Hinderlich für die Funktion als Recheneinheit ist zudem die große Zahl von Nullen, die sich bei der Umrechnung ergeben, so kostet beim heutigen Wechselkurs das 50 Cent-Brötchen rund 0,0005 Bitcoin. Aufgrund des rein digitalen Charakters der KW ist dies indes ein lösbares Problem, die Skalierung ließe sich unschwer auf ein für die Konsumenten leichter handhabbares Maß verändern.

### **Relative Stärken der Kryptowährungen**

Um sich dauerhaft als Zahlungsmittel durchzusetzen, müssen KW zumindest bezüglich einzelner Eigenschaften als „besser“ eingestuft werden als die bisherigen Währungen bzw. Zahlungsmethoden. Ein erster primär makroökonomischer Gesichtspunkt ist die schon angesprochene Wertstabilität. Die bisherige Währungsgeschichte ist zu einem großen Teil eine Geschichte von Untergängen, wieder und wieder wurden von den Regierungen Währungen über Inflationen wertlos gemacht. Die Auslagerung der Geldpolitik auf eine regierungsunabhängige Zentralbank ist eine vergleichsweise junge Entwicklung, die hier einen Riegel vorgeschoben hat. Aber die Zentralbankunabhängigkeit lässt sich per Gesetz schnell wieder ändern, sie ist fragil. Zudem können auch unabhängige Zentralbanken eine unsolide Geldpolitik betreiben.

Kryptowährungen überwinden diese Probleme rigoros. Zumindest bis dato erfolgt die Ausgabe von KW ausschließlich durch Private, keine Regierung und keine andere Zentralinstanz ist hier involviert. Der Anreiz zur Inflationierung durch Private (ein häufig vorgebrachtes Argument gegen den privaten Währungswettbewerb à la Hayek) entfällt aus zwei Gründen. Zum einen gibt es keine private Einzelperson, die die KW emittiert, die neu geschaffenen Währungseinheiten fallen an diejenigen, die eine kryptografische Aufgabe als

---

<sup>10</sup> Vgl. M. Rysman und S. Schuh: New Innovations in Payments, NBER Working Paper No. 22358, Juni 2016.

erstes lösen. Dieser Prozess des Mining erfolgt nach transparenten und für alle einsehbaren Regeln, jeder kann grundsätzlich an diesem Prozess teilnehmen. Zum anderen wird über die Höhe des Geldangebots nicht diskretionär entschieden, sondern das Geldangebot folgt über die Lösung der kryptografischen Aufgaben mehr den Regeln der Mathematik. Beim Bitcoin ist das Angebot auf rund 21 Millionen Einheiten begrenzt, eine Inflationierung des Bitcoins ist damit definitiv ausgeschlossen. Andere KW wie der Peercoin fixieren das Angebot nicht in absoluter Höhe, sondern lassen auch langfristig eine positive Wachstumsrate zu. Dass die Bindung an mathematische Regeln aus ökonomischer Sicht nicht uneingeschränkt sinnvoll ist, wird weiter unten noch diskutiert werden.

Auf der mikroökonomischen Ebene erlaubt die Blockchain-Technologie die Umgehung traditioneller Finanzintermediäre, gerade Geschäftsbanken droht eine Erosion ihrer Geschäftsmodelle. Ähnlich wie beim Peer-to-Peer-Lending, wo unter Nutzung von Plattformen Kreditgeber auf direktem Weg finanzielle Ressourcen an Kreditnehmer transferieren, können mittels der Blockchain Überweisungen direkt zwischen Zahlern und Zahlungsempfängern vorgenommen werden. Die Technologie gewährleistet, dass bei einem gewünschten Geldtransfer von Frau A zu Herrn B nur Herr B der tatsächliche Empfänger sein kann, dass Frau A nachweislich über das entsprechende Guthaben verfügt und dass der Betrag tatsächlich von Frau A kommt. Eine vertrauenswürdige dritte Person oder Institution wie die Geschäftsbank, die diese Fragen für Frau A und Herrn B bis dato klärt, ist nicht vonnöten.

Die von den traditionellen Finanzintermediären erhobenen Bearbeitungs- bzw. Überweisungsgebühren erlauben eine grobe Abschätzung des Einsparpotentials. Den Extrempunkt bilden grenzüberschreitende Überweisungen, dort betragen die Gebühren durchschnittlich 8,9 Prozent des Überweisungsbetrags.<sup>11</sup> Bei Kreditkartenunternehmen wie Visa und Mastercard sind 2 bis 3 Prozent des Umsatzes als Gebühr zu zahlen, PayPal erhebt eine Gebühr von 1,9 Prozent des Verkaufswerts plus 0,35 € pro Transaktion. Diesen Einsparungen sind indes die Gebühren gegenüberzustellen, die Bitcoin-Zahlungsdienstleister wie BitPay oder Coinbase beim Umtausch von traditionellen Währungen in Bitcoin et vice versa verlangen, derzeit rund 1 Prozent des Umtauschbetrags. Ob Bitcoin-Geschäfte ihren heutigen Kostenvorteil dauerhaft behalten, wird mitunter unter Hinweis auf vermutlich ansteigenden Transaktionsgebühren in Frage gestellt.<sup>12</sup> Die derzeit dominierende Entlohnung der Miner in Form von neuen Bitcoins wird als Reflex des immer komplexer werdenden

---

<sup>11</sup> Goldman Sachs: All About Bitcoin, in: Global Market Research, Issue 21, März 2014. Aufgrund eines intensiven Wettbewerbs und regulatorischer Initiativen bspw. auf Ebene der EU sind die Gebühren in jüngerer Zeit etwas gesunken.

<sup>12</sup> Vgl. N. Houy: The Economics of Bitcoin Transaction Fees, in: GATE Working Paper No. 1407, Februar 2014.



Mining-Prozesses ersetzt werden müssen durch Gebühren, über deren Höhe zum jetzigen Zeitpunkt nur spekuliert werden kann.

Ein unstrittiger Pluspunkt: Über die Blockchain bzw. das Bitcoin-System abgewickelte Transaktionen haben einen Geschwindigkeitsvorteil. Auf traditionellem Weg vorgenommene Überweisungen dauern innerhalb der EU einen Werktag, bei Überweisungen in die USA rund fünf Werktage und bei Überweisungen in Entwicklungsländer bis zu 20 Werktage. Dies ist anachronistisch. Beim Bitcoin-System müssen die jeweiligen Informationen (Sender, Betrag, Empfänger etc.) in einem Block aufgenommen werden, die Erzeugung eines Blocks dauert ungefähr zehn Minuten. Eine Transaktion gilt üblicherweise nach sechs Blöcken als bestätigt, mithin sind Transaktionen innerhalb einer Stunde als sicher zu betrachten. Beim Litecoin reduziert sich die Zeitdauer auf rund 15 Minuten. Die Reaktion der Zentralbanken auf diese technologische Entwicklung ließ ein wenig auf sich warten, aber derzeit arbeiten sie intensiv an der Entwicklung von Instant Payment Systems, die diesen Nachteil der bankmäßigen Abwicklung des Zahlungsverkehrs zumindest abmildern.<sup>13</sup>

### **Sicherheitsaspekte**

Wenn sich KW durchsetzen sollen, müssen sie ihren Nutzern ein Maß an Sicherheit bieten, welches zumindest mit den traditionellen Währungen vergleichbar ist. Dies bedeutet insbesondere, dass Transaktionen fälschungssicher sein müssen. Im Wesentlichen lassen sich die Risiken eines KW-Systems in zwei Gruppen einteilen: Risiken, die innerhalb des Netzwerks entstehen, und Risiken, die an der Schnittstelle, also bei der Verwendung des Netzwerks entstehen. Zu den inneren Risiken gehören die Sicherheit der Kryptographie, die Deanonymisierung von Nutzern, die Möglichkeit des double spending und Sicherheit des Konsensusalgorithmus.

Im direkten Vergleich überwiegen unseres Erachtens die Schnittstellenrisiken. In der bisher rund achtjährigen Nutzung der Bitcoin-Blockchain sind bis dato keine substantiellen technischen Fehlfunktionen bekannt geworden, und auch wenn die Sicherheit der Kryptographie ein grundsätzliches Problem ist<sup>14</sup>, die von Nakamoto gewählte Verschlüsselungstechnik ist (bisher) als sicher einzustufen.

Intensiv diskutiert ist das Konzept der Pseudonymität, das Transaktionen für Dritte nicht einsehbar machen soll. Bargeld bietet die „perfekte“ Anonymität gegenüber Außenstehenden,

---

<sup>13</sup> Vgl. M. Tompkins und A. Olivares: Clearing and Settlements Systems from Around the World: A Qualitative Analysis, in: Bank of Canada Staff Discussion Paper 2016-14, Juni 2016.

<sup>14</sup> Vgl. dazu z.B. Vgl. z.B. I. Giechaskiel, C. Cremers und K. B. Rasmussen: On Bitcoin Security in the Presence of Broken Crypto Primitives, IACR Cryptology ePrint Archive, 2016, 167.

nur die am Tausch unmittelbar Beteiligten sind involviert. Den Gegenpol bilden herkömmliche Banküberweisungen, bei denen die Einsichtnahme und das Zurückverfolgen von Transaktionen zumindest für die jeweilige Bank unproblematisch sind, die Weitergabe bspw. an staatliche Behörden wie das Finanzamt ist kaum zu unterbinden. KW beschreiten hier einen Mittelweg: alle Transaktionen sind auf der Blockchain festgehalten und für alle Netzwerkteilnehmer öffentlich einsehbar. Aber die Transaktionen liegen nur unter Pseudonymen vor. Sie sind lediglich durch Zahlungsadressen identifiziert, die durch ein private-public-key-Paar erzeugt werden. Diese verhindern in erster Instanz eine Identifikation der Nutzer, auch wenn eine völlige Deanonymisierung – zumindest unter gewissen Voraussetzungen – nicht ausgeschlossen werden kann.<sup>15</sup>

Hervorgehoben wird zudem oft die Möglichkeit von 51%-Angriffen auf das Bitcoin-System: es gilt die Blockchain, die von der Mehrheit der Rechenleistung akzeptiert wurde. Verfügt ein Angreifer über diese Mehrheit, kann er rückwirkend Blöcke und damit auch eigene Transaktionen verändern. Kurzum, der Angreifer kann entscheiden, welche Transaktion in der Blockchain abgebildet wird.<sup>16</sup> Dadurch unterliegt das Netzwerk einem systemimmanenten Risiko. Allerdings sind die hierfür notwendigen Rechnerkapazitäten heute derart umfangreich und damit kostenintensiv, dass dieses Risiko als gering einzustufen ist. Eine Neubewertung ist ggf. erforderlich, sollte es zu einer noch stärkeren Konzentration bei den Mining Pools kommen.

Deutlich kritischer für die Sicherheit ist die Schnittstellen-Problematik. Die Mehrzahl der KW-Transaktionen erfolgt unter Zuhilfenahme von Zahlungsdienstleistern, die die Umwandlung von traditionellen Währungen in KW et vice versa vornehmen, die in einer Online-Wallet den Private Key speichern etc. Der KW-Nutzer greift hier also auf einen Dritten zurück, dem er – ähnlich einer Geschäftsbank – vertrauen muss. Auch im KW-System treten also Intermediäre auf. Diese sind nicht nur ein potentiellles Angriffsziel, sondern können selbst in betrügerischer Absicht handeln. Die Konsequenz ist das Risiko eines entsprechenden Vermögensverlustes. Bei traditionellen Finanzintermediären tritt dasselbe Problem auf, das KW-System ist diesbezüglich bedingt eine Verbesserung, da es die Verwendung von Intermediären zumindest zum Teil obsolet werden lässt und keinen dauerhaften Einsatz von Intermediären voraussetzt. Zu einer ähnlichen Einschätzung gelangt man bei Geschäften mit kleinen Transaktionsvolumina. Hier wollen Kunden wie Händler in

---

<sup>15</sup> Vgl. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker und S. Savage, a.a.O. und A. Biryukov, D. Khovratovic und I. Pustogarov: Deanonymisation of Clients in Bitcoin P2P Network, in: CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, S. 15 – 29.

<sup>16</sup> Vgl. S. Nakamoto, a.a.O.

der Regel nicht warten, bis die Transaktion in der Blockchain bestätigt ist, gerade der Händler trägt damit ein Restrisiko. Dies gilt grundsätzlich auch bei Kartenzahlungen, aber hier gibt es – anders als bei KW-Systemen – Versicherungslösungen, die das Risiko eines Zahlungsausfalls begrenzen.

Ein wesentlicher Vorteil von KW ist die Abwesenheit von Falschgeld. Jeder Nutzer kann, basierend auf der Kenntnis der gesamten Transaktionshistorie, prüfen, ob eine Transaktion valide ist und sie (ggf. nach einer Wartezeit bzw. wenn die Transaktion durch eine gegebene Zahl von Blöcken bestätigt wurde) akzeptieren. Um die Sicherheit der Transaktionshistorie zu gewährleisten, werden bestimmte Referenzblöcke fest im Quellcode des Bitcoin-System festgehalten und damit final fixiert.<sup>17</sup>

Da KW letztlich softwaregesteuert sind, lassen sich Risiken und Sicherheitslücken nicht mit letzter Sicherheit eliminieren. Dies gilt jedoch im selben Maße für die traditionellen Zahlungssysteme, sodass zusammenfassend festzuhalten bleibt, dass KW in Bezug auf das Thema technische Sicherheit traditionellem Geld nicht nachstehen, sondern möglicherweise sogar überlegen sind, sofern die Nutzer entsprechende Rahmenbedingungen einhalten.

### **Regionale Verteilung des Bitcoins**

Kryptowährungen kennen keine Staatsgrenzen und keine regionalen oder geographischen Hindernisse, die die Nutzung einschränken. Ihr digitaler Charakter erlaubt eine denkbar einfache globale Verwendung. Gleichwohl ist für nationale Akteure das Ausmaß der regionalen Verwendung von KW von großem Interesse, denn die regionale Verteilung gibt Auskunft darüber, wie intensiv sie von den KW tatsächlich betroffen sind. Zu nennen sind hier bspw. die deutschen Geschäftsbanken, für die die Intensivierung des Wettbewerbs vehement ist, wenn KW-Transaktionen in Deutschland eine weite Verbreitung finden. Analoges gilt für nationale Behörden wie die BaFin, die ggf. aufsichtsrechtlich einschreiten muss, da sie KW-Transaktionen als Finanzinstrumente in der Form von Rechnungseinheiten eingestuft hat. Oder die Geldpolitik: Die Europäische Zentralbank könnte die KW praktisch ignorieren, wenn Bitcoin & Co. nicht im Euroraum, sondern fast ausschließlich in China oder den USA Verwendung finden würden.

Bei einer regionalen Einordnung muss zwischen der Schaffung und der Nutzung der KW unterschieden werden. Die Schaffung der wichtigsten KW, dem Bitcoin, lässt sich anhand der Daten des Mining-Prozesses regional lokalisieren. Mindestens 99% der Blöcke auf der Bitcoin-Blockchain werden durch Mining Pools erstellt. Dabei zeigt sich eine

---

<sup>17</sup> Vgl. z.B. I. Giechaskiel, C. Cremers und K. B. Rasmussen, a.a.O.

zweifache Konzentration: Die fünf größten Pools erzeugen zusammen etwa 80% der Blockchain-Blöcke, und vier von diesen fünf Mining Pools operieren (wegen der niedrigen Energiepreise) von der VR China aus. Entsprechend ist der chinesische Renminbi die bedeutsamste Währung im Bitcoin-Handel (31%), gefolgt vom US-Dollar (25%) und dem Euro (9%).<sup>18</sup>

Die Zuordnung der Nutzer zu bestimmten Ländern gestaltet sich im Vergleich zur Schaffung des Bitcoins ungleich schwieriger, da das System pseudonym ist und somit kein zentrales Verzeichnis existiert, mit dessen Hilfe die Regionalstruktur studiert werden könnte. Mithin müssen andere Datenquellen genutzt werden. Eine erste Informationsquelle ist die Verteilung der weltweit derzeit 126 Handelsplätze.<sup>19</sup> Eine klare regionale Schwerpunktsetzung lässt sich nicht identifizieren, die Bitcoin-Börsen verteilen sich über den gesamten Erdball, 37 Börsen finden sich in Asien, 35 in Europa, 19 in Nordamerika, 13 in Südamerika, 12 in Australien/Ozeanien und 3 in Afrika. Das Land mit den meisten Bitcoin-Handelsplätzen ist das Vereinigte Königreich mit 19 Börsen gefolgt von der VR China mit 12 Börsen und den USA mit 9 Börsen. Deutschland ist mit einer Börse eher Bitcoin-Entwicklungsland.

Betrachtet man die Downloadhäufigkeit der Bitcoin-Software als Approximation der Bitcoin-Nutzung, so sind die USA, die VR China, Deutschland, das Vereinigte Königreich, Kanada und die Niederlande als Hauptnutzungsgebiete zu identifizieren.<sup>20</sup> Korrigiert man diese Zahlen für die unterschiedlichen Bevölkerungsgrößen, ergibt sich jedoch ein etwas anderes Bild: es sind insbesondere die skandinavischen Länder und ihre Nachbarn, die eine höhere Ausbreitung des Bitcoins aufweisen, also eben jene, die schon jetzt – relativ betrachtet – eine weniger ausgeprägte Affinität zum Bargeld besitzen.

### **Utopia: eine reine Kryptowährung-Welt**

Kryptowährungen haben heute eine Marktkapitalisierung von rund 20 Mrd. Euro, das entspricht 0,3% der Euro-Geldmenge M1. Die Zentralbanken inkl. der EZB beobachten daher die Entwicklungen bei den KW, aber als unmittelbare „Bedrohung“ werden sie nicht wahrgenommen. Diese Einschätzung mag sich auch mittelfristig als richtig erweisen, wenn die besagte kritische Masse an Nutzern nicht überschritten wird. Dann wären KW eher

---

<sup>18</sup> Vgl. Europäische Zentralbank: Virtual Currency Schemes – a Further Analysis, Februar 2015.

<sup>19</sup> Vgl. Exchange War: List of Crypto-Exchanges, <http://www.exchangewar.info> (06.03.2017).

<sup>20</sup> Vgl. dazu für eine Analyse der Bitcoin-Nodes auch: J. A. Donet Donet, C. Pérez-Solà und J. Herrera-Joancomartí: The Bitcoin P2P network, in: R. Böhme, M. Brenner, T. Moore und M. Smith (Hrsg.): Financial Cryptography and Data Security, FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers, Berlin 2014, S. 87 – 102.

vergleichbar mit der Vielzahl von Regionalwährungen („Chiemgauer“, „Bürgerblüte“ etc.), deren Rückwirkungen auf die geldpolitische Ausrichtung als vernachlässigbar anzusehen sind.

Aber die Einschätzung kann falsch sein. Zur Skizzierung der Implikationen ist es illustrativ, sich den anderen Grenzfall vorzustellen: eine reine KW-Welt. Angenommen, es gäbe ausschließlich Bitcoins. Eine reine Bitcoin-Welt wird durch Deflation gekennzeichnet sein. Dies ist anhand der Quantitätsgleichung  $MV = PY$  schnell skizziert. Beim Bitcoin ist die umlaufende Geldmenge  $M$  technologisch auf rund 21 Mio. Bitcoins begrenzt. Sofern plausiblerweise die Umlaufgeschwindigkeit des Geldes  $V$  nicht fortlaufend ansteigt, muss bei steigendem Einkommen  $Y$  das Preisniveau  $P$  fallen. Bisher ist weitgehend unerforscht, wie sich eine Volkswirtschaft mit inhärent angelegter Deflation verhält. Die Anlageform „Geld“ erhält eine positive Realverzinsung, womit sich der Zinsabstand zu anderen Kapitalanlageformen zumindest verringert. Die Erwartung sinkender Preise mag eine Verschiebung der Güternachfrage in die Zukunft zur Folge haben, sodass kurzfristig negative Output-Effekte resultieren. Das Szenario einer deflationären Ökonomie lässt sich umgehen, wenn die digitale Währung nicht mengenmäßig beschränkt ist, sondern auch im Gleichgewicht eine positive Wachstumsrate aufweist. Dies ist bspw. beim Peercoin gegeben, was ad hoc aus geldtheoretischer Sicht als überlegene Alternative erscheint.

Der Realwert einer KW wie dem Bitcoin wird heute gemessen mit Hilfe des Wechselkurses zum Euro oder US-Dollar. Sind für einen Bitcoin mehr US-Dollar zu zahlen, so steigt c.p. der Realwert des Bitcoins. Werden im Extremfall die staatlichen Währungen vollständig verdrängt, so stellt sich das Problem der Ermittlung eines adäquaten Preisindex. Was ist der Realwert eines Bitcoins in einer reinen Bitcoin-Welt? Möglich wäre die Bildung eines harmonisierten Konsumentenpreisindex, der den Preis eines im Weltmaßstab repräsentativen Warenkorb widerspiegelt. Gegeben die im Weltmaßstab massiven Unterschiede in den nationalen Präferenz- und damit Konsumstrukturen wäre ein solcher Index indes weitgehend inhaltsleer. In Analogie zum Euroraum bietet sich als Alternative die Verwendung nationaler Indices an, womit der Realwert des Bitcoins dann von Land zu Land unterschiedlich definiert ist. Die Formulierung aller Preise in derselben Währungseinheit erleichtert die Vergleichbarkeit der Preise, die ökonomisch relevantere Bestimmung der Realwerte ist dagegen unvermindert komplex.

Die Welt als Ganzes ist definitiv kein optimaler Währungsraum im Sinne von Mundell. Das Beiseitelegen des nominalen Wechselkurses als Instrument zur Beeinflussung des realen Wechselkurses und erst recht das Beiseitelegen der nationalen Geldpolitik ist im Euroraum

schon umstritten, im Weltmaßstab wäre es abstrus. Dieses Faktum beantwortet die Frage, ob Utopia im Sinne einer reinen KW-Welt überhaupt erstrebenswert ist, mit einem klaren „nein“. Auch ein Wettbewerb mehrerer KW würde hieran nichts ändern, denn die sich einstellenden Wechselkurse zwischen den jeweiligen KW hätten nichts mit den ökonomisch notwendigen Anpassungen zwischen zwei Ländern oder Ländergruppen zu tun. Sollten KW in einem wettbewerblichen Prozess die traditionellen Währungen zum Teil verdrängen, so spricht dies für einen Effizienzgewinn, die resultierende Marktlösung ist grundsätzlich zu begrüßen. Eine vollständige Verdrängung hingegen würde mit dem Verlust von unzweifelhaft erforderlichen Stabilisierungsinstrumenten einhergehen. Aus makroökonomischer Perspektive ist daher der Fortbestand traditioneller Währungen mit traditioneller Geldpolitik der reinen KW-Welt vorzuziehen.

### **Kryptowährungen und Zentralbankpolitik**

Beide Extremszenarien – KW bleiben ein Randphänomen bzw. sie verdrängen die traditionellen Währungen vollständig – erscheinen unrealistisch. Zu rechnen ist mit einer dauerhaften Koexistenz von KW und traditionellen Währungen. Die makroökonomischen Implikationen einer solchen Koexistenz sind bis dato weitestgehend unerforschtes Terrain. Eine nennenswerte Ausnahme ist die an der Bank of England entstandene Studie von Barrdear und Kumhof.<sup>21</sup> Die Autoren integrieren eine KW in ein DSGE-Modell, wobei das Verhältnis von Kryptowährung und Zentralbankgeld qua Annahme fixiert ist, sodass Geldpolitik als stabilitätspolitisches Instrument erhalten bleibt. Ein interessantes Ergebnis ihrer Analyse: die Implementierung der KW wirkt wie ein Wachstumsmotor, langfristig ist der Output in einer reinen KW-Welt rund 3% höher als in der Welt ohne KW. Hanl und Schwanebeck kommen zu einem ganz ähnlichen Ergebnis.<sup>22</sup> Durch die KW verbessert sich der Prozess der Finanzintermediation, das Zusammenfinden von Sparern und Investoren ist mit weniger Reibungsverlusten verbunden, der gleichgewichtige Realzins vermindert sich, die Kapitalbildung wird forciert.

Die KW beeinflusst nicht nur das langfristige Gleichgewicht, sondern auch das Anpassungsverhalten einer Volkswirtschaft auf makroökonomische Schocks. Ein erster Punkt betrifft die vom Bitcoin-Erfinder Nakamoto genannte Korrektur von geldpolitischen Fehlern,

---

<sup>21</sup> J. Barrdear und M. Kumhof: The Macroeconomics of Central Bank Issued Digital Currencies, in: Bank of England Staff Working Paper No. 605 (2015).

<sup>22</sup> A. Hanl und B. Schwanebeck: Financial Intermediation and Bitcoin: Using Bitcoin as Alternative Investment Vehicles, Präsentation beim DLT Workshop der Universität Kassel im März 2017, [https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IVWL/Michaelis/Kryptow%C3%A4hrungen\\_als\\_Geld\\_der\\_Zukunft\\_korrigiert.pdf](https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IVWL/Michaelis/Kryptow%C3%A4hrungen_als_Geld_der_Zukunft_korrigiert.pdf).

d.h. die traditionelle Geldpolitik wird weniger als Stabilisator denn als Störquelle oder Schockverstärker angesehen. Wie Hanl und Schwanebeck zeigen, wirkt die KW in der Tat wie ein Puffer, geldpolitische Schocks bspw. in Form eines unerwarteten Zinsanstiegs werden in ihren Auswirkungen auf Output, Konsum und Investitionen abgemildert. Durch die KW entsteht ein Substitut für traditionelle Bankgeschäfte, sodass die geldpolitisch induzierte Verteuerung der Bankkredite eine Ausweichreaktion in Richtung KW, also eine verstärkte Finanzintermediation über den Kryptowährungskanal, impliziert.

Die Kehrseite der Medaille: die Geldpolitik verliert an Effizienz. Wenn der Rückgang der Investitionen infolge eines Zinsanstiegs kleiner ausfällt, büßt das Zinsinstrument an Wirksamkeit ein. Kommt es zu Schocks in der Güternachfrage und/oder im Güterangebot, deren Output- und Inflationseffekte von Seiten der Geldpolitik abzufedern sind, so ist die optimale Reaktion der Geldpolitik auf die verminderte Effizienz ein verstärkter Einsatz des Zinsinstruments. Die Geldpolitik wird durch den KW-Kanal also aggressiver agieren.<sup>23</sup>

Weil die Forschung der Interaktion von KW und Geldpolitik erst am Anfang steht, sind diverse Probleme schlicht als offen zu bezeichnen. Dies gilt zum Beispiel für die veränderte Rolle der Geschäftsbanken im Transmissionsprozess der Geldpolitik. Geht die verstärkte Finanzintermediation mittels KW mit einer verstärkten Wanderung in den Bereich der Schattenbanken einher, so werden nicht zuletzt die Regulierungsbehörden hier aktiv werden. Dies gilt gleichermaßen für etwaige Auswirkungen auf die Finanzmarktstabilität. Die Rolle der Geldpolitik als Lender of last resort ist neu zu überdenken. Erwähnt sei zudem, dass KW selbst als Verursacher von Schocks auftreten können. Der Zusammenbruch einer Plattform wie Mt. Gox, der mit dem Verlust von 650.000 Bitcoins einherging, wäre ein Ereignis mit realwirtschaftlichen Auswirkungen, das eine Reaktion der Zentralbanken erzwingen würde.

### **Schlussbetrachtung**

Kryptowährungen haben den engen Zirkel der Computer-Nerds verlassen, sie sind heute lebendiger Bestandteil des Finanzmarktgeschehens. Entsprechend gilt es ihre Funktions- und Wirkungsweise zu verstehen, was aufgrund des recht komplexen technologischen Hintergrunds nicht ganz einfach ist. Sofern technische Weiterentwicklungen die Handhabung weiter erleichtern, haben sie das Potential zu einem allgemein akzeptierten Zahlungsmittel. Noch ist dies nicht der Fall, aber die Zentralbanken sind gut beraten, wenn sie das dynamische Feld der Kryptowährungen auf ihre Forschungsagenda setzen und versuchen, die Folgen für

---

<sup>23</sup> Dies ist analog zum sog. Kostenkanal der Geldpolitik, vgl. J. Palek und J. Michaelis: Optimal Monetary Policy in a Currency Union: Implications of Country-specific Financial Frictions, in: Credit and Capital Markets. 49. Jg. (2016), H. 1, S 1 – 36.

die geldpolitische Konzeption sowie für die Wirkungsweise des traditionellen Instrumentensets zu antizipieren.

Dass Kryptowährungen nicht als vorübergehender Hype anzusehen sind, liegt maßgeblich an der technologischen Neuerung der Blockchain, nach dem Internet eventuell „the next big thing“.<sup>24</sup> Für die Zentralbanken ist die unmittelbare Folge eine massiv verstärkte Konkurrenz im Bereich der Zahlungssysteme. Wenn ein großer Teil der (grenzüberschreitenden) Zahlungen Peer-to-Peer erfolgt, können Zentralbanken die Stabilität des Zahlungsverkehrs nicht mehr im selben Ausmaß gewährleisten. Einige Zentralbanken nehmen die Herausforderung aktiv an und denken darüber nach, die Blockchain-Technologie für sich selber zu nutzen durch die Herausgabe einer eigenen digitalen Währung.<sup>25</sup>

---

<sup>24</sup> Vgl. W. Blocher, a.a.O.

<sup>25</sup> Vgl. B. Fung und H. Halaburda: Central Bank Digital Currencies: A Framework for Assessing Why and How, in: Bank of Canada Staff Discussion Paper 2016-22, November 2016.