

Krypto-Währungen Sicherung von Währungs-Konkurrenz ?

reeter.context:ökonomie

2019.01

>Krypto-Währungen<

Sicherung von Währungs-Konkurrenz ?

Wolfgang Reeder

R.Hasse/H.Schneider/K.Weigelt (Hrsg.):
Lexikon Soziale Marktwirtschaft
Online Version 2019

Funktionen des Geldes

Arbeitsteiliges Wirtschaften braucht ein allgemeines Tausch-Mittel, eine Rechen-Einheit, ein Wertaufbewahrungs-System: braucht Geld (=> *W.Reeder: Geld, Sozialbindung und Freiheit (1)*): Münzen, Geldscheine. Geldscheine sind zunächst einmal Schuldscheine, Bescheinigung eines Anspruchs an einen Schuldner. Wirtschaftlicher Verkehr wird wesentlich erleichtert, wenn solche Schuldscheine allgemein gültig sind, ein allgemeiner Anspruch an Güter und Leistungen. Allgemeingültigkeit ermöglicht eine Instanz, die für allgemeingültige Regeln menschlichen Umgangs zuständig ist: der Staat. Geld ist deshalb im Lauf der Geschichte eine staatliche Einrichtung geworden - mit einem schwerwiegenden Problem: Auch die Repräsentanten des Staates brauchen für ihr Handeln Geld. Wenn sie für die Herstellung des Geldes, von Münzen und Scheinen zuständig sind, können sie in Versuchung geraten, den Materialwert von Münzen zu verringern, die Zahl und den Nennwert von Scheinen zu erhöhen - heute sagen wir: einfach Geld zu drucken. Dieser Versuchung sind Regierungen immer wieder erlegen. Mit zunehmender Zahl und steigendem Nennwert von Geldscheinen sinkt die Kaufkraft des Geldes, wenn die Menge an Gütern und Leistungen nicht in demselben Umfang steigt - wir sprechen von Inflation (gegenwärtig - 2017/18/19 - von Vermögenspreis-Inflation): Geld verliert mehr und mehr seine Wertaufbewahrungs-Funktion.

Die Menschen streben deshalb immer wieder nach einem allgemeinen Tausch-Mittel, das seine Wertaufbewahrungs-Funktion erhält. Das erklärt das Interesse an Gold. Zu Zeiten

der kommunistischen Herrschaft war D-Mark ein begehrtes Zahlungsmittel in Ostdeutschland und Ost- und Südost-Europa. Wir können sagen: Die D-Mark war eine Konkurrenz-Währung, trat in Wettbewerb mit den dortigen Währungen. Daraus können wir eine Folgerung ziehen, die *Friedrich August von Hayek* 1976 in radikalster Form als Forderung nach "Denationalisation of Money" (*London: Institute of Economic Affairs* 1976 (2)) formulierte: die Zulassung von Währungs-Konkurrenz, von privaten Währungen. Wenn wir Geld-Scheine als Schuld-Scheine betrachten, sehen wir, dass es in offenen Marktwirtschaften immer möglich war und ist, mit 'privatem Geld' zu operieren. Solche Schuld-Scheine sind nur eine Frage der Geltung, der Akzeptanz: Wie viele Wirtschafts-Subjekte akzeptieren sie als Zahlungsmittel ? Gold ist ein Wertaufbewahrungs- und deshalb auch wirksames Zahlungsmittel, weil ihm allgemeine Geltung zukommt und weil die Menge in etwa überschaubar begrenzt ist. Ein Zahlungsmittel, dessen Menge erkennbar begrenzt und dessen Herkunft nachvollziehbar ist, könnte ähnlich attraktiv sein. Die Nachvollziehbarkeit der Herkunft jedenfalls ist mit der => *Blockchain*-Technik gegeben.

Krypto-Währungen Beispiel BitCoin

Sind Krypto-Währungen dieses Zahlungsmittel ? Das griechische Wort 'Kryptós' bedeutet 'verborgen', 'versteckt' (und kryptisch nennen wir unklare, schwer verständliche Aussagen). Um die Funktionsweise von Krypto-Währungen zu bestimmen, müssen wir 'Geld' noch genauer bezeichnen. Denn die meisten Zahlungen leisten wir nicht mit Scheinen und Münzen, sondern über Veränderungen der Zahlen auf Konten bei unseren Banken. Diese Zahlen nennen wir im Unterschied zu Bar-Geld Buch-Geld. BitCoin, eine der Krypto-Währungen können wir ebenso wenig in der Geldbörse haben wie BuchGeld. BuchGeld sind Beträge in den Büchern, heute

den Computern der Banken. Sehen wir uns die Schritte unserer Verfügung über BuchGeld und der Verfügung über eine Krypto-Währung an, und zwar die bekannteste, den BitCoin.

Bank-Konto-Eröffnung: Wir eröffnen bei einer Bank ein Online-Konto - mit Nutzer-Name, Passwort, Bestätigungs-Mail mit Empfangs-Bestätigung

BuchGeld: Wir bekommen eine Konto-Nummer und einen verschlüsselten Zugang, heute meist noch PIN, eine Persönliche Identifikations-Nummer. Für eine Transaktion verwenden wir eine einmalige Transaktions-Nummer TAN. Auf unserem Konto erscheinen Zahlungen-Eingänge und Zahlungen-Ausgänge.

Buchgeld-Überweisung: Bei einer Transaktion, durch eine Zahlung wird der Betrag auf unserem Sender-Konto verringert, wird der Betrag auf dem Empfänger-Konto erhöht: auf beiden Konten erscheint ein entsprechender neuer Saldo.

BitCoin-Wallet-Eröffnung: Auf einem BitCoin-Marktplatz eröffnen wir ein Wallet (eine elektronische Geldbörse) - mit Nutzer-Name, Passwort, Bestätigungs-Mail mit Einmal-Pass-Wort.

BitCoin: Wir bekommen eine BitCoin-Adresse, per Zufalls-Auswahl aus Buchstaben und Zahlen generiert - offen (wie unser Bank-Konto bei Überweisungen) und einen persönlichen Schlüssel aus Buchstaben und Zahlen - geheim. Auf unserer BitCoin-Adresse erscheinen nicht Summen oder Salden, sondern es erscheint ein Block der vorherigen Transaktion.

BitCoin-Transaktion: Auf unserer BitCoin-Adresse und allen anderen BitCoin-Adressen der betroffenen User wird an den Block der vorherigen Transaktion der aktuelle Block angehängt. Der Block enthält nur die Transaktion (nicht den Saldo), enthält: Input - voriger Block, Sender-Adresse, Anzahl BitCoin, Output - Empfänger-Adresse. Der Block wird an das BitCoin-Netzwerk gesendet, wird dort von 'BitCoin-Miners' mit hochkomplexen Rechen-Operationen verifiziert, d.h. auf Übereinstimmung mit allen bisherigen Blocks getestet. Bei erfolgreicher Verifikation wird

der Block an die Transaktions-BlockChain angehängt, sonst wird er gelöscht. Alle Blocks erscheinen in einem allgemein aufrufbaren Register, der einschlägigen BlockChain.

Zahlungs-Verkehr ist beim *BuchGeld* möglich entsprechend Kontostand und Verfügungs-Rahmen einschließlich Überziehungs-Kredit mit jedem Betrag. Belege können erzeugt und ausgedruckt werden.

Zahlungs-Verkehr ist beim BitCoin nur entsprechend verfügbaren BitCoins möglich. Bei ungleicher Input- und Output-Menge wird die Übertragung in mehrere Transaktionen zerlegt. BitCoin ist teilbar: ein Satoshi (3) entspricht einem Hundertmillionstel BitCoin. Beleg-Funktion ist derzeit - Dez.2018 - in Arbeit.

Manipulation, Diebstahl ist beim *BuchGeld* möglich durch verschiedene Methoden des Konto-Hacking.

Manipulationen würden beim *BitCoin* auf allen beteiligten Rechnern als nicht-autorisierte Block-Änderung erkennbar und gelöscht, erscheinen also als ausgeschlossen. Diebstahl durch Hacking ist schwierig, kommt aber vor.

Währungs-Konkurrenz

Mit Krypto- oder Virtuellen Währungen sind also alternative Währungen entstanden, wie sie von Verfechtern der Währungs-Konkurrenz immer wieder gefordert wurden und werden. Marktwirtschaft ist eben ein offenes System, das grundlegende soziale Innovationen ermöglicht. Wer dem Wert der heimischen Währung nicht traute, hatte in marktwirtschaftlichen Systemen - sofern es keine Kapitalverkehrs-Kontrollen gab - immer schon die Möglichkeit, sein Geld in anderen Währungen oder in Gold anzulegen. Konvertibilität von Währungen ist eine Form von Währungs-Konkurrenz. Sie gibt Wirtschafts-Subjekten die Freiheit, eine Währung zu verlassen, wenn ihre Wert-Entwicklung unsicher wird.

Virtuelle Währungen scheinen darüber hinaus nun gleich zwei wesentliche Probleme unseres Geld-Systems zu lösen: (1.) die beliebige

Vermehrbarkeit 'gesetzlicher Zahlungsmittel' und (2.) die Transaktions-Kosten der Übertragung von Geld-Beträgen.

Problem Transaktions-Kosten

Transaktion-Kosten: Überweisungen von BuchGeld sind ein mehrstufiger Vorgang: Überweisungsauftrag an Bank A, Abbuchung bei Bank A, Daten an Giro-Netz / Rechenzentrum der Banken-Gruppe A, Daten von Rechenzentrum an Clearing-Stelle, Daten von Clearingstelle an Giro-Netz Bank B, Betrag einbuchen in Kunden-Konto bei Bank B, Konto-Auszug an Kunden. Bei virtuellen Währungen fallen drei Arbeitsschritte an: Block-Erstellung und Block-Anhang User A, Verifikation durch Miner, Block-Information und Block-Anhang User B.

Allerdings: Virtuelle Währungen der Blockchain-Technik beruhen auf hoch-komplexen Berechnungen mit schnell zunehmendem Ressourcen-Bedarf: der Strom-Verbrauch einer einzigen Bitcoin-Transaktion belief sich Ende 2017 auf 222 Kilowatt-Stunden. Bei zunehmender Zahl - Bitcoin-Transaktionen Ende 2017: 400.000 täglich - erhöhen sich auch zudem die Transaktions-Zeiten. Die inzwischen äußerst komplizierte Produktion (Mining) von Bitcoins, wegen der benötigten Energie-Menge in großen Server-Farmen überwiegend in China und der Mongolei angesiedelt, verursacht dort einem Ausstoß von 8 bis 13 Tonnen CO₂ je Bitcoin. (*Digiconomist (Alex de Vries): Bitcoin Sustainability Report December 2017. Digiconomist 2018.01(4).*)

Problem Währungs-Stabilität

Währungs-Reform im Sinne von Währungs-Konkurrenz: Krypto-Währungen wurden in der Folge der Finanz-Krise entwickelt. In der Finanz-Krise zeigten sich die zerstörerischen Folgen weitgehend unregulierter Geld-Schöpfung der Banken - genauer: ihrer Kredit-Schöpfung: die Finanz-Krise (wie auch die => *Euro-Krise*) war und ist eine Schulden-Krise, ermöglicht durch (a) mangelhafte staat-

liche Regulierung und (b) durch staatliche Verschuldung selbst. Das provozierte die Suche nach einem Zahlungsmittel ohne die Risiken des staatlich legitimierten Geldes. Krypto-Währungen haben in der Tat den gravierenden Vorteil einer exakt begrenzten Geld-Menge - Bitcoins sind durch ihren Entstehungs-Algorithmus, ihre komplexe Rechen-Formel auf 21 Millionen begrenzt. Steigende Nachfrage bei streng begrenzter Menge bewirkt Preis-Steigerung, ja: Preis-Explosion.

Damit wird Bitcoin zu einem Anlage-, genauer: zu einem Spekulations-Objekt, zu einem Gegenstand von Wetten auf steigende oder fallende Kurse. Das Kriterium Limitierung, Begrenzung mag für die Menge von Bitcoin gelten - für die durch Spekulation, durch Wetten gebildeten Preise scheint es nicht zu gelten. Und: Unaufhörlich werden neue Krypto-Währungen produziert. Auf rund eintausend wird ihre Anzahl Ende 2017 veranschlagt. Als allgemeines, universell einsetzbares Tausch-Mittel, Zahlungs-Mittel, als allgemein geltende Rechen-Einheit sind sie absehbar nicht geeignet. Einige wenige davon werden bleiben. Ob sie das gegenwärtig vorherrschende Banken-gestützte Geld-System verdrängen können, scheint fraglich.

Gefahren von Krypto-Währungen

Fraglich ist nicht nur, ob Krypto-Währungen das tradierte Geld-System verdrängen können. Fraglich ist auch, ob dies erstrebenswert ist. Drei Probleme sind offensichtlich: (a) Der Algorithmus, das Rechensystem, mit dem Bitcoin eingeführt wurde und Bitcoins geschaffen werden können, begrenzt deren Zahl, macht sie damit für die täglich Milliarden Transaktionen untauglich, prädestiniert sie zum Spekulations-Objekt. (b) Der Energie-Bedarf für Computer und Server steht im Widerspruch zu zwingend notwendigen Bemühungen, den Verbrauch natürlicher Ressourcen zu verringern. (c) Der hohe Energie-Bedarf bewirkt schon heute eine räumliche Konzentration der Server auf wenige Regionen. Fortschreitende Konzentration läuft dem Anspruch zuwider, ein konsequent dezentralisiertes System einzuführen. Mit Zentralisie-

rung von Server-Farmen entsteht eine Gefahr, die jeder Konzentration innewohnt: dass letztlich doch Manipulationen möglich werden.

Nun wirkt Wettbewerb als Entdeckungsverfahren (*Hayek*) auch bei Krypto-Währungen. Neue, alternative oder ergänzende Systeme, auch mit weiteren Funktionen werden produziert. Die Markt-Kapitalisierung aller noch existierenden Krypto-Währungen - viele verschwinden bald wieder - belief sich im November 2017 auf 305 Mrd.US-Dollar (*Motley Fool* <www.fool.de> 03.12.2017 (5)). Manche dieser Systeme verringern die BitCoin-Probleme erheblich. So gilt für *Lite Coin*, 2013 programmiert: (a) Das System arbeitet schneller, verbraucht damit (b) wesentlich weniger Energie. (c) Wie BitCoin ist Lite Coin auf Basis einer geometrischen Reihe programmiert. Die Rate, mit der die Krypto-Währungen generiert werden können, sinkt in vorgegebenen Zeit-Intervallen - so wird die Menge begrenzt: bei LiteCoin auf das Vierfache - 84 Millionen - der BitCoin-Menge. (d) LiteCoin arbeitet mit einem Verifikations-(Proof of Work) Algorithmus (<https://litecoin.org/>) (6), der Zentralisierungstendenzen und damit auch letztendlich doch drohenden Manipulations-Gefahren entgegenwirken soll.

Ob das gelingt, ob also Krypto-Währungen sicherer sind vor Manipulation und Verwässerung als unser tradiertes Geld-System, können wir angesichts immer neuer Bedrohungen von Cyber-Sicherheit in Frage stellen. Und: Schon der Prozess tradierter Geld-Schöpfung, der Entstehung des Fiat-Geldes (des durch Kredit-Gewährung der Banken entstehenden Geldes und des persönlichen Beitrages dazu) ist für ökonomisch nicht wenigstens rudimentär Vorgebildeten oft nicht nachvollziehbar. Nun ist auch die Vielzahl von Krypto-Währungen, ihr Entstehen und Vergehen kaum noch übersehbar. Vor allem die höchst komplizierten Rechen-Systeme der Erzeugung dieser Währungen und ihres Einsatzes für Transaktionen machen sie nur für hochqualifizierte IT-Spezialisten durchschaubar - und für ihre Produzenten oft zu einer sprudelnden Reichtums-Quelle. Ohnmachts-Gefühle von Normal-Bürgern gegen-

über dem Geld-System werden nicht verringert, sondern eher verstärkt.

Effizienz, Transparenz, Universalität, Stabilität sind Bedingungen des Transaktions-Mediums Geld. Transparenz ist nur für eine enge Experten-Gemeinschaft gegeben. Notwendigkeit und Effizienz-Vorteile von Universalität zeigen sich in der Einführung einer Gemeinschafts-Währung, wenn nicht wesentliche ökonomische Voraussetzungen - wie bei der Einführung des Euro (=> *Euro-Krise*) - missachtet werden.

Marktwirtschaft: offenes System

Verbleiben Effizienz und Stabilität als Kriterien für die Leistungs-Fähigkeit eines Geld-Systems, also Optimierung der Transaktions-Kosten und Stabilisierung der Wertaufbewahrungsfunktion.

Gesamtwirtschaftlich können wir mit einer ökonomisch fundierten Währungs-Union Transaktions-Kosten wesentlich senken. Einzelwirtschaftlich gilt das für Online Banking und Mobile Payment im Rahmen einer Währungs-Union, gestützt auf =>SEPA und =>TARGET - the Single Euro Payments Area, den Einheitlichen Euro-Zahlungsverkehrsraum und the Trans-European Automated Real-time Gross Settlement Express Transfer System, das Transeuropäische automatische Echtzeit-Brutto-Express-Abwicklungssystem.

Für die Stabilisierung der Wertaufbewahrungsfunktion des Geldes sind zwei Bedingungen wesentlich, die in der Tat anhaltend durch politische Prozesse gefährdet sind: Die Geldschöpfungs-, genauer: Kreditschöpfungsmöglichkeit der Banken muss realwirtschaftlich orientiert reguliert, d.h. begrenzt werden. Notwendige Begrenzung der Kreditschöpfung ist auch zu beziehen auf deren wichtigste Quelle: die Staats-Verschuldung. Dazu ist eine Verfassungsrechtlich verankerte Schulden-Bremse zwingend. Werden diese beiden Bedingungen realisiert, ist Stabilisierung des tradierten Geld-Systems möglich.

Krypto-Währungen kommen in Marktwirtschaften eine wichtige Funktion zu, besonders bei verbreiteten Zweifeln am tradierten Geld-System. Krypto-Währungen demonstrieren, dass grundlegende Alternativen, grundlegende Innovationen, auch in Gestalt alternativer Geld-Systeme in Marktwirtschaften als offenen, Wettbewerbs-orientierten Systemen möglich sind.

Wenn (a) marktwirtschaftliche Offenheit, also die bürgerliche Entscheidungs-Freiheit für alternative Geld-Systeme - wie den Krypto-Währungen - erhalten bleibt, und soweit es (b) unterschiedliche Währungen mit freien, staatlich nicht manipulierten Wechselkursen gibt, bleibt Währungs-Konkurrenz auch im tradierten Geld-System gesichert.

(1) Grundlegend zur Ökonomie des Geldes:

(a) Wolfgang Reeder: Geld, Sozialbindung und Freiheit. Bonn 1991

www.w-reeder.de/pdfarchiv/Geld_Sozial_bindg_Freiheit.pdf

(b) Thomas Mayer: Die neue Ordnung des Geldes. München 2014

(2) Friedrich August von Hayek: Denationalisation of Money. London 1976

<https://mises.org/library/denationalisation-money-argument-refined>

(3) Das Konzept BitCoin wurde 2008 unter dem offensichtlichen Pseudonym Satoshi Nakamoto publiziert: Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin Foundation. 11.2.2008

<https://bitcoin.org/bitcoin.pdf>

(4) Digiconomist (Alex de Vries): Bitcoin Sustainability Report December 2017. Digiconomist 2018.01.

<https://digiconomist.net/bitcoin-sustainability-report-12-2017>

(5) The Motley Fool (David u. Tom Gardner): Bitcoins größter Konkurrent ist nicht Ethereum. Berlin 12.2017.

<https://www.fool.de/>

(6) <https://litecoin.org/>