Der Bitcoin Wahn

09.02.2018 | Markus Mezger

Eines vorneweg. Dieser Artikel bemüht sich nicht um Ausgewogenheit oder Objektivität. Der Leser wird nicht viele Formulierungen finden, die dem Schema "Einerseits … Andererseits" gehorchen. Vielmehr ist dieses Papier ein Pamphlet. Eine Philippika, die sich gegen offensichtliche Ausplünderung von leichtgläubigen Anlegern richtet.

Der Autor dieser Zeilen war bis vor wenigen Monaten der Meinung, dass das törichte Verhalten einzelner Anleger mit der Internetblase um die Jahrtausendwende einen nicht mehr zu übertreffenden Gipfel erreicht hat. Damals schossen "Internetunternehmen" wie Pilze aus dem Boden. Viele ohne jede Aussicht auf nachhaltige Gewinne. Anleger zeichneten blind überteuerte Aktienemissionen, getrieben von dem Wunsch nach schnellen Reichtum.

Erwachsene Menschen saßen tagelang vor ihren Computern, um via Internet sekundengenau zu jeder vollen Stunde eine Zeichnung von Internetaktien abzugeben, um durch eine Zuteilung auch einen Zipfel des sagenhaften neuen Reichtums zu erhaschen. IT-Experten wurden die neuen Superstars der Finanzbranche. Einzelne von ihnen erklärten eine Zielrendite von 20% per annum auf das Kapitalvermögen als antiquiert. Unternehmen aus der sogenannten Old Economy galten als hochgradig langweilig.

Aber ich habe mich geirrt. Es geht noch schlimmer. Viele Umstände rund um das Thema Bitcoin werden Anlegern aus der Zeit der Internetaktienblase bekannt vorkommen. Einzelne Elemente des Bitcoins-Systems scheinen jedoch noch perfider ausgestaltet. Dazu gehören der Kettenbriefcharakter des Systems, der den Initiatoren riesige Seignoragewinne aus der Schöpfung der ersten Bitcoins ermöglicht hat. Dass sie nach dem Platzen der Blase von wütenden Anlegern zur Rechenschaft gezogen werden könnten, mag den Gründern des Bitcoin-Systems wohl bewußt gewesen sein. Sonst wäre es wohl kaum nötig gewesen, sich hinter Pseudonymen verstecken.

Bis heute ist die Identität der Initiatoren des Bitcoin-Systems nicht zweifelsfrei festgestellt.

Nun könnte man es mit der Feststellung einer Blase bewenden lassen und sich anderen, wichtigeren Themen zuwenden. Wie das Internet hat aber auch das Thema Bitcoin einige Innovationen hervorgebracht, die die Preisblase überleben könnten. Dabei sollte zwischen Bitcoin als Zahlungsmittel und der dahinterstehenden Verschlüsselungstechnologie unterschieden werden.

Bei der Beschäftigung mit dem Thema habe ich festgestellt, dass es reichlich Lektüre gibt, die sich mit der Frage beschäftigt, wie man in Bitcoin investiert und welche Punkte bei der Anwendung des Systems zu beachten sind. Wer in diesem Artikel einen Leitfaden für eine Investition in Bitcoin erwartet, braucht gar nicht weiterzulesen. Der Artikel richtet sich vielmehr an Leser, die sich fragen, ob der Bitcoin eine sinnvolle Innovation ist und ob er dem selbstgesteckten Anspruch, sich als Bargeldersatz und Wertaufbewahrungsmittel zu etablieren, gerecht werden kann.

Die Idee hinter Bitcoin

Die Grundidee hinter Bitcoin läßt sich leicht nachvollziehen. Die letzten 20 Jahre waren in den globalen Geldsystemen von noch nie da gewesenen Verwerfungen geprägt. Ausgangspunkt dieser Entwicklung war das Platzen der japanischen Aktienblase im Jahr 1990. Die japanische Fiskal- und Geldpolitik reagierte mit den bis dahin bewährten Maßnahmen aus Konjunkturprogrammen und monetären Stimuli. Nur schlugen diese Maßnahmen in Nippon selbst nicht mehr an. Dafür um so mehr in den USA und Europa, wohin das in Japan neugeschaffene Zentralbankgeld abgeflossen war.

Während die Konsumgüterpreise den Währungshütern weltweit nur geringe Inflationsgefahren suggerierten, geriet die Welt der Assetpreise vor dem Hintergrund des billigen und reichlichen Geldangebots zunehmend außer Kontrolle.

Die Notenbanken in den USA und Europa hatten aus den Erfahrungen Japans die falschen Schlüsse gezogen. Hochmütig erklärte der damalige US-Notenbankpräsident Ben Bernanke im Jahre 2002, dass die USA mit Hilfe der Notenpresse nicht in eine japanische Nullzinsfalle geraten könne. Aber trotz aller Bemühungen von "Helikopter-Ben" landeten die USA wenige Jahre später gerade dort. Die Notenbanken hatten ein Wechselspiel aus billigem Geld und Assetpreisblasen geschaffen.

Der Versuch, die nach dem Platzen der Blasen unvermeidlichen Krisen mit noch billigerem Geld zu bekämpfen, erinnert an die Geschichte Münchhausens, der sich an den eigenen Haaren aus dem Sumpf zu ziehen gedachte. Die Notenbanken trifft jedoch keineswegs die Alleinschuld. Eine expansive Notenbankpolitik ist eine notwendige, aber keine hinreichende Bedingung für Preisblasen. Die Gleichschaltung vieler Anleger und ein kollektiver Wahn müssen noch hinzukommen. Mit der Computerisierung des Wertpapierhandels und einer Vielzahl quantitativer, prozyklischer Anlagestrategien ist auch diese Bedingung zunehmend erfüllt gewesen.

Bis vor 10-15 Jahren unterlagen einzelne Anleger der Illusion, dem Platzen von Preisblasen zuvorkommen zu können, indem sie ihre Papiere rechtzeitig verkauften und dafür Kasse in Form von Kontoguthaben hielten (auch wenn dies für alle Anleger im Aggregat natürlich niemals gelingen kann). Mit der Krise des Jahres 2008 war auch der Nimbus der Sicherheit dieser Strategie gefallen. Im Gegensatz zu Bargeld handelt es sich bei Bankguthaben eben nicht um von den Zentralbanken geschaffenes Geld, sondern nur um einen Rechtsanspruch auf die Auszahlung desselben.

Dieser Anspruch steht und fällt mit dem Wohl und Wehe der kontoführenden Banken. Kollabieren diese, ist auch das Guthaben verwirkt. Die Sicherungssysteme sind im Ernstfall vermutlich nicht das Papier wert, auf dem sie stehen. Außerdem droht bei allen Giroguthaben latent die Gefahr, dass sie über Nacht gesperrt werden und ein Transfer nicht mehr möglich ist. Wie politische Sanktionen (Rußland, Venezuela) oder die Krise in Griechenland zeigen, kann das nicht mehr als ein rein theoretischer Fall abgetan werden.

Blieb als Alternative für die Krisenprävention nur die Hortung von Bargeld oder Edelmetallen. Ersteres hat den Vorteil, dass Zahlungen anonym vorgenommen werden können, während bei elektronischen Transaktionen zumindest der kontoführenden Bank Verbrauchs- und Verhaltensgewohnheiten offengelegt werden müssen. In Zeiten zunehmenden Datendiebstahls könnten die Daten aber auch noch wo ganz anders landen.

Die Anonymität im Goldhandel ist seit einigen Jahren vorbei, auch wenn die Behörden bei einer Großzahl der historisch angehäuften privaten Goldbestände noch immer im Dunkeln tappen. Beide Geldformen haben aber den Nachteil, dass ein erhöhter Aufwand für die Absicherung gegen Diebstahl und Verlust getrieben werden muß. Größere Bestände dürfen nicht ohne vorherige Anmeldung über Landesgrenzen hinweg transportiert werden.

Aus diesen Beschränkungen hat sich die Idee entwickelt, ob es nicht ein Geld geben könne, das von den Währungsbehörden nicht gesperrt werden kann und das von überall aus elektronisch über alle Landesgrenzen hinweg transferiert werden kann. Eine Geldform, die nicht von der wackligen Existenz einer Bank abhängt und gleichzeitig die Funktion eines Wertaufbewahrungsmittels erfüllt, da seine Kaufkraft nicht durch die unkontrollierte Schaffung zusätzlicher Geldeinheiten entwertet werden kann.

Ein Zahlungsmittel, mit dem Geldtransfers anonym vorgenommen werden können, ohne Verhaltens- und Verbrauchsdaten offenzulegen. Mit einem Wort ein Geld, das die Vorteile des elektronischen Zahlungsverkehrs mit den Vorteilen von Bargeld/Gold kombiniert.

Aus diesen Ideen heraus wurde der Bitcoin geboren und es ist natürlich kein Zufall, dass er auf dem Höhepunkt der Finanzkrise des Jahres 2008 lanciert wurde. Mitte September 2008 war die Investmentbank Lehman Brothers pleite gegangen. Nur wenige Wochen später, am 31.10.2008, wurde ein Papier mit dem Titel "Bitcoin - A Peer-to-Peer Electronic Cash System" veröffentlicht. Als Autor ist das Pseudonym Satoshi Nakamoto angegeben. Bis heute ist nicht geklärt wer sich hinter diesem Pseudonym verbirgt. Die Initiatoren des Bitcoin-Systems waren clever genug, ihren bzw, ihre Namen der Öffentlichkeit vorzuenthalten, da das System von Anfang an zugunsten der Insider der ersten Stunde ausgestaltet war.

Ausgestaltung und Funktionsweise des Bitcoin-Systems

Für die Verbuchung elektronischer Geldtransfers gibt es grundsätzlich zwei Möglichkeiten. Entweder wird ein Transaktionsregister von einer damit beauftragten, zentralen Organisation geführt. In der Bundesrepublik Deutschland ist die Deutsche Bundesbank per Gesetz mit der Organisation des Zahlungsverkehrs für das gesetzliche Zahlungsmittel Euro beauftragt. Eine zentrale Registerführung birgt jedoch die Gefahr, dass Regierungen Geldtransfers blockieren können, indem sie die mit der Registerführung beauftragte Organisation kontrollieren. Geldtransfers sind dann nur möglich, solange sie politisch opportun sind.

Das Bitcoin-Netzwerk hat die zweite Variante, eine dezentrale Registerführung gewählt. Das Bitcoin-System soll ein freies Netzwerk gleichberechtigter Nutzer sein (Peer to Peer Netzwerk). Geldtransaktionen bzw. der Transfer von Bitcoins werden von der Gemeinschaft der Netzwerkteilnehmer validiert und protokolliert.

Das klingt idealistisch, wirft aber in der Praxis einige wichtige Fragen auf: Wer prüft bei einer dezentralen Organisation, ob ein Nutzer überhaupt über ausreichend Guthaben verfügt, um einen Transfer zu tätigen? Warum sollte sich jemand den Aufwand machen, fremde Transaktionen zu prüfen und zu protokollieren? Was hat er davon? Und schließlich: Wenn viele Nutzer gleichzeitig ein Transaktionsregister führen, wie kann sichergestellt werden, dass es nicht zu Datenkonflikten durch gleichzeitige Zugriffe kommt? Wie kann ein für jeden Nutzer einheitliches und eindeutiges Transaktionsregister sichergestellt werden?

Ich will zunächst diesen Fragen nachgehen, weil durch deren Klärung auch die Antwort auf die wichtigste aller Fragen, nämlich die wie ein Bitcoin überhaupt geschaffen wird, gegeben wird. Die Prüfung der Berechtigung, einen Bitcoin-Transfer vornehmen zu können, erfolgt über eine verschlüsselte Signatur. Sie ist ein Kernstück der Bitcoin-Technologie. Jeder Bitcoin-Netzwerkteilnehmer verfügt über einen privaten Schlüssel, der nur ihm bekannt ist (er wählt eine Zahl mit bis zu 78 Stellen), und einen für andere Teilnehmer sichtbaren öffentlichen Schlüssel, der aus dem privaten Schlüssel errechnet wird. Details seien Ihnen an dieser Stelle erspart.

Wichtig zu wissen ist lediglich, dass die Rechenoperation nicht umgekehrt werden kann. Aus dem sichtbaren öffentlichen Schlüssel können also keinerlei Rückschlüsse auf den privaten Schlüssel gezogen werden. Da der öffentliche Schlüssel eine unhandlich lange Zahl ist, hat sich in der Praxis anstelle des öffentlichen Schlüssels die wesentlich kürzere Bitcoin-Adresse durchgesetzt. Die Bitcoin-Adresse wird mit einer mathematischen Funktion (doppelte Hash-Funktion) aus dem öffentlichen Schlüssel errechnet.

Die Bitcoin-Adressen sind die Pseudonyme der Netzwerkteilnehmer. Will ein Netzwerkteilnehmer einen Transfer von Bitcoin-Einheiten durchführen, so versendet er eine Transaktionsnachricht, seinen öffentlichen Schlüssel und eine dazu passende zweiteilige Signatur an andere Netzwerkteilnehmer. Sobald diese die Nachricht empfangen haben, können sie durch mathematische Funktionen die Signatur entcodieren und überprüfen, ob die Signatur zum mitgegebenen öffentlichen Schlüssel paßt. Gleichzeitig können Netzwerkteilnehmer überprüfen, ob die Bitcoin-Adresse, die als Sender angegeben ist, über ein entsprechendes Guthaben verfügt.

Für jede Bitcoin-Transaktion muß eine Bitcoin-Adresse für den Sender und eine Bitcoin-Adresse für den Empfänger angegeben sein. Das Bitcoin-System enthält keine Bestände, sondern eine vollständige Liste aller jemals stattgefundenen Bitcoin-Transaktionen. Daraus ist für jeden Netzwerkteilnehmer öffentlich einsehbar, welche Bitcoin-Einheiten zu welchem Zeitpunkt von einer Bitcoin-Adresse zu einer anderen Bitcoin-Adresse geflossen sind. Ein Traum für jeden Notenbanker, wenn so etwas bei Bargeld möglich wäre.

Stellen Sie sich vor, jeder Bargeldschein würde von der Notenbank mit einem Chip ausgestattet, der Ihre Fingerabdrücke verzeichnet und den Zeitpunkt, wann er von wem zu wem geflossen ist. Zwar nicht mit Namen und Adresse, aber immerhin unter Angabe eines Pseudonyms. Daraus ließen Praxiswerte über Umlaufgeschwindigkeit, Ausgabe- und Investitionsverhalten gewinnen, die andernfalls oft mühsam geschätzt werden müssen. Aber nicht nur für Geldpolitiker ist das ein Traum, sondern auch für alle im Handel tätigen Unternehmen, deren Datenneugier ja ohnehin schon kaum zu bremsen ist.

Wenn Sie zu einem Netzwerk wie Bitcoin Zuflucht nehmen, dann ist es vermutlich das Letzte, was Sie wollen, dass alle Netzwerkteilnehmer jede einzelne Ihrer Geldüberweisungen, und wenn auch nur unter einem Pseudonym, verfolgen können. Also werden Sie viele Pseudonyme generieren, zwischen denen Sie wie ein Hütchenspieler so lange Bitcoins hin und herschieben bis für Außenstehende ihre tatsächlichen Transaktionen nicht mehr nachvollziehbar sind. Die Verwaltung von vielen Pseudonymen, die aus privaten und öffentlichen Schlüssel berechnet wurden, wird schnell unübersichtlich.

Deswegen übernimmt ein Programm, Wallet (Brieftasche) genannt, die Verwaltung der "Guthaben", die ihnen unter den verschiedenen Pseudonymen, bzw. Bitcoin-Adressen zugeschrieben sind. Teilweise wird für jede Transaktion von Bitcoin-Einheiten eine neue Bitcoin-Adresse generiert. Beispielsweise könnte es sein, dass Sie eine Ware verkauft haben und einer Ihrer Bitcoin-Adressen dafür ein ganzer Bitcoin gutgeschrieben wurde. Nun möchten Sie für den Kauf einer anderen Sache aber nur einen halben Bitcoin ausgeben.

Die Wallet spaltet den ganzen Bitcoin, den Sie erhalten haben (Transaktionsinput) in zwei Transaktionen zu je einem halben Bitcoin auf (Transaktionsoutput): eine zugunsten der Bitcoin-Adresse des Verkäufers und eine zugunsten einer neuen Bitcoin-(Wechselgeld)Adresse. Die Teilnahme am Bitcoin-System ist also alles andere als trivial. Bitcoin wird das Bargeld oder einfache Kontoüberweisungen nicht ersetzen können. Noch wird es in der Breite Online-Überweisungen ersetzen können. Für die überwiegende Mehrheit der Bevölkerung sind Bitcoin-Transfers aufgrund ihrer Komplexität nicht geeignet. Dem Wachstumspotenzial von Bitcoin sind enge Grenzen gesetzt. Dies sollte man bei einer Investition im Hinterkopf haben.

Aber kommen wir zu den Transaktionsvorschlägen zurück, die einzelne Netzwerkteilnehmer an andere propagieren. Prinzipiell ist die Überprüfung der Signatur für jeden Teilnehmer machbar. Dies verursacht jedoch nicht zu vernachlässigende Kosten für Rechnerhardware und Strom, da allein für die

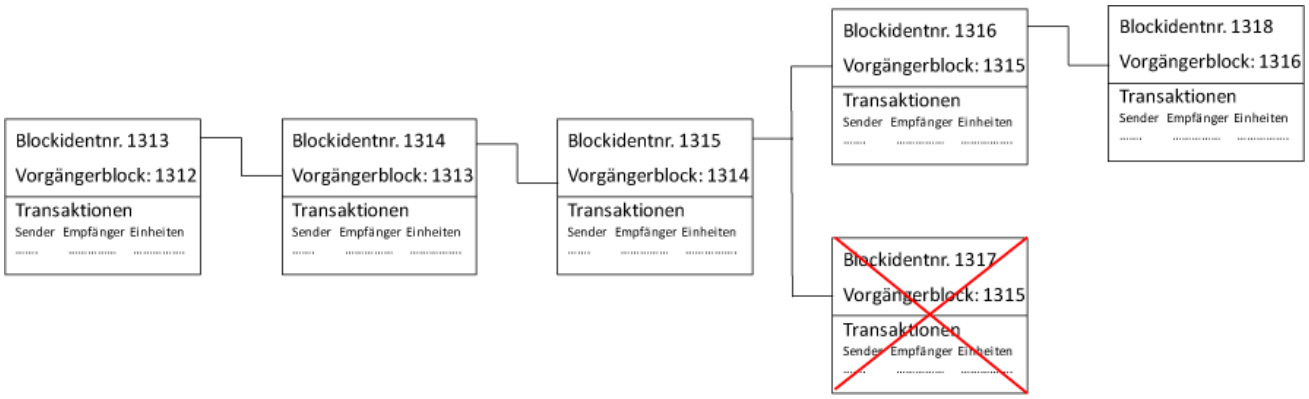
Verifizierungsfunktion eine Kopie des kompletten Transaktionsregisters auf dem eigenen Rechner gespeichert werden muß (der Speicherplatzbedarf liegt zum 1. Februar 2018 bei knapp 150 Gigabyte, Tendenz weiter steigend).

Zudem sollen eingehende Transaktionsnachrichten im Netzwerk laufend weiterverbreitet werden. Wenn neben der Generierung durch die Wallet Transaktionen auch noch verifiziert und verbucht werden können, dann spricht man von einem vollwertigen Knoten (Full Node) des Bitcoin-Netzwerks. Aber warum sollte sich jemand den Aufwand machen, den Rechner permanent laufen zu lassen, um die Transaktionsnachrichten Dritter zu verbreiten, ihre Signatur zu überprüfen oder sie gar in einem aufwendigen Verfahren in die Transaktionsliste aufzunehmen? Die Antwort ist verblüffend: Weil man durch neugeschaffene Bitcoin-Einheiten dafür entlohnt wird.

Bitcoins werden nämlich wie jede Form des Fiat-Money aus dem Nichts geschöpft. Und zwar für die Teilnehmer des Bitcoin-Netzwerks, die Transaktionen in der öffentlichen Transaktionsliste festhalten. Diese besteht aus aufeinander aufbauenden Transaktionsblöcken (Blockchain). Jeder Block, in dem mehrere neue Transaktionen gebündelt sind, hat eine eindeutige Blockidentifikationsnummer. Gleichzeitig ist im Blockkopf (Block Header) auch die Blockidentifikationsnummer des Vorgängerblocks vermerkt. So entsteht eine wachsende Kette von Blocks mit allen jemals getätigten Transaktionen, die sich eindeutig referenzieren.

Da es für die Fertigung eines neuen Blocks neue Bitcoins gibt, wollen möglicherweise viele Netzwerkteilnehmer die Kette gleichzeitig erweitern. Die Folge wäre eine Kette, die sich immer mehr verzweigt und in denen Transaktionen ggf. doppelt festgehalten sind.

Das Bitcoin-Netzwerk versucht diese Problematik mit zwei Ausgestaltungsmerkmalen zu lösen. Erstens haben sich die Bitcoin-Netzwerkteilnehmer zu dem Konsens zusammengefunden, dass nur der längste Zweig, also der Zweig mit der größeren Anzahl von Blocks zum letzten eindeutigen Vorgängerblock, fortgesetzt wird. Der andere Zweig wird verworfen. Die Netzwerkteilnehmer, die diesen Zweig gefertigt haben, gehen leer aus, während die Schöpfer des längeren Zweiges ihre volle Entlohnung in Form neuer Bitcoins erhalten.



Die Problematik der Verzweigung besteht natürlich insbesondere dann, wenn viele Netzwerkteilnehmer gleichzeitig in Sekundenschnelle neue Blocks an die Blockkette anfügen können. Deswegen wurde als zweite Maßnahme im Bitcoin-Netzwerk ein künstlicher Schwierigkeitsgrad für die Erstellung eines gültigen Blocks eingeführt. Im Bitcoin-Netzwerk kann ein neuer Blockkandidat nur dann an die Blockkette angefügt werden, wenn seine Blockidentifikationsnummer einem bestimmten, vom Bitcoin-Netzwerk vorgegebenen Schwellenwert, genügt. Die Netzwerkteilnehmer wetteifern darum, als Erster das Schwellenwertkriterium zu erfüllen.

In der Praxis variieren sie bestimmte Parameter für die Generierung alternativer Blockidentifikationsnummern. Das Ganze wird dann Mining genannt, um eine (nicht angebrachte) Analogie zum Schürfen von Edelmetallen herzustellen. Überhaupt sind viele Begriffe aus dem Marketing von Gold entlehnt, um das Thema Bitcoin zu verkaufen. Aber das ist ein anderes Thema. Jedenfalls ist der Prozeß des "Mining" wirklich kompliziert. Begriffe wie "Iteration des Nonce-Werts" oder "alternative Merkle-Root" sind für viele Menschen jenseits des kognitiven Fassungsvermögens.

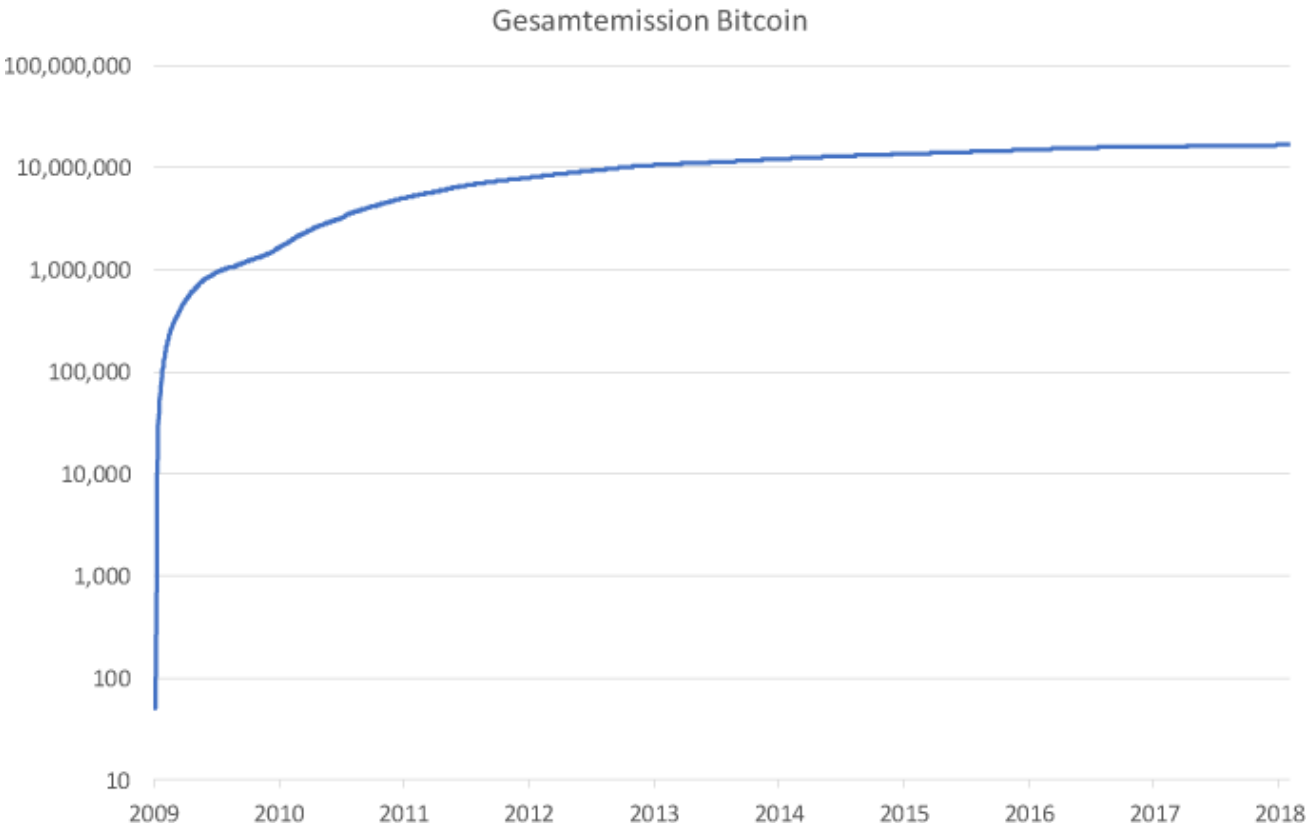
Die Schöpfung neuer Bitcoins ist also IT-Spezialisten mit speziellen Kenntnissen vorbehalten. Heute versuchen Vereinigungen von erfahrenen Netzwerkteilnehmern (Mining-Pools) mit hochgerüsteten Serverfarmen, vorwiegend in Asien, die hochgeschraubten Schwierigkeitsgrade zu lösen. Der Einzelkämpfer mit normaler IT-Ausrüstung hat praktisch keine Chance mehr, neue Bitcoins zu ergattern. Ein Großteil der

bisher geschöpften Bitcoins dürfte zu Beginn auf das Konto der Leute geflossen sein, die dieses System ersonnen haben.

Aber es kommt noch schlimmer. Das Bitcoin-System war am Anfang nur ein paar Nerds bekannt, die sich den Spaß machten, so etwas einmal technisch auszuprobieren. Ende des Jahres 2008 war Bitcoin ein elektronisches Spielgeld, das an neue Nutzer oft verschenkt wurde. Die erste Preisschätzung im Oktober 2009 ergab einen Wert von 0,000764 USD. Die erste Warentransaktion soll im Mai 2010 stattgefunden haben. Dabei wurden 10.000 Bitcoin für den Gegenwert von zwei Pizzen bezahlt. Mit dem heutigen Kurs von rund 10.000 USD je Bitcoin hätten die beiden Pizzen etwa 100 Millionen Dollar gekostet. Bei wenigen Netzwerkteilnehmern war am Anfang die Verzweigung der Blockkette durch gleichzeitiges Anfügen von Blocks kaum zu befürchten.

Dementsprechend brauchte man auch keinen hohen künstlichen Schwierigkeitsgrad für die Erzeugung neuer Blocks, während die Erzeugung heute mit sehr hohen Rechner- und Stromkosten verbunden ist (s.u.). Aber die Blockerstellung war nicht nur wesentlich einfacher, sie wurde auch noch wesentlich besser vergütet. Zu Beginn wurden noch 50 Bitcoin-Einheiten als Kompensation für die Blockerstellung gezahlt, heute sind es 12,5 Einheiten. Dieser Wert wird nach der Fertigstellung einer bestimmten Blockanzahl immer weiter halbiert bis er sich asymptotisch der Null nähert. Die Anzahl der insgesamt zu emittierenden Bitcoins soll so auf 21 Millionen beschränkt werden.

Diese Beschränkung und eine schrumpfende Entlohnung bei steigendem Aufwand führen langfristig zu massiven Anreizproblemen zur Aufrechterhaltung des Systems (s.u.). Das Ganze ist ein großer Kettenbrief: Ein kleiner Kreis von hochspezialisierten IT-Fachleuten nimmt für eine an sich triviale Dienstleistung (Transfer von Geldeinheiten) hohe Beträge ein, während die Nachfolgenden bei steigendem Aufwand immer geringer kompensiert werden. In der logarithmischen Darstellung der Entwicklung aller bisher geschaffenen Bitcoin kann man klar erkennen, dass die großen Wachstumsraten in der Bitcoin-"Geld"menge zu Beginn des Systems erzielt wurden, als das Ganze nur wenigen Insidern bekannt war.



Quelle: https://blockchain.info/de/charts/total-bitcoins, eigene Darstellung, Stand 1.2.2018

Aber nicht nur unfreiwillige, sondern auch mutwillige Verzweigungen der Blockchain sind denkbar. Wie oben angesprochen, setzt sich bei einer Verzweigung der längere Zweig durch. Der kürzere wird aufgegeben. Was aber passiert, wenn ein Teilnehmer versucht, andere Blöcke zu unterdrücken, indem er einen längeren Zweig an die Blockchain anzufügen versucht? Ein solcher Teilnehmer müßte über eine im Vergleich zu seinen Mitbewerbern sehr große Rechenkapazität verfügen, damit er in der Lage ist, mehrere gültige Blöcke hintereinander zu erstellen.

So ein Angriff auf das Bitcoin-Netzwerk wäre dann einigermaßen aussichtsreich, wenn ein Teilnehmer mehr als die Hälfte der gesamten Rechenleistung des Bitcoin-Netzwerks kontrollieren würde. Man spricht deswegen auch vom 51%-Angriff. Der Teilnehmer könnte zwar keine Transaktionen verändern, da er die Signatur nicht fälschen kann. Aber er kann willkürlich entscheiden, welche Transaktionen in die Blockchain aufgenommen werden und welche nicht. Ein Bitcoin-Käufer wäre in diesem Fall nicht mehr von einer Notenbank oder einer anderen Behörde abhängig, dafür aber von einem dominanten Netzwerkpaten.

Einen echten Vermögensschaden könnten derjenige erleiden, der sich darauf verläßt, dass eine Transaktion zu seinen Gunsten verbucht wird. Zum Beispiel der Verkäufer eines Goldbarrens, der dafür drei Bitcoin erhalten soll. Generiert der Käufer neben der ersten Transaktion noch eine zweite, die das gleiche Bictoin-Guthaben (Transaktionsinput) referenziert und die zu seinen Gunsten lautet, gibt es zwei widersprüchliche Transaktionen.

Das gleiche Geld wurde sozusagen doppelt ausgegeben (Double Spend). Nur eine der beiden Transaktion kann in die Blockchain aufgenommen werden. Ein dominanter Netzwerkteilnehmer könnte dafür sorgen, dass die zweite und nicht die erste Transaktion an die Blockchain angefügt wird. Der Verkäufer des Goldbarrens ginge dann leer aus. Dumm nur, wenn er den Goldbarren schon ausgehändigt hat. Der Bitcoin eignet sich demnach wenig für Geschäfte im Einzelhandel, bei denen Ware gegen Cash gilt.

Nun ist ein 51%-Angriff umso unwahrscheinlicher, je mehr Anreize für einen gesunden Wettbewerb beim "Mining" bestehen. Beim gegenwärtigen Bitcoin-Kurs konkurrieren noch mehrere Mining-Pools darum, sich die nächsten Bitcoin-Einheiten zu verdienen. Gegenwärtig gilt eine Transaktion, die in einem Block steht, der mindestens sechs Nachfolger hat, praktisch als unumkehrbar. Wie seht das aber aus, wenn die Vergütung immer weiter sinkt und die Preise fallen, weil sich die Netzwerkteilnehmer zu anderen Kryptowährungen abwenden oder ganz aus Kryptowährungen aussteigen?

Kann ein gutgläubiger Bitcoin-Käufer dann tatsächlich sicher sein, dass nicht eine Gruppe mit großem IT-Budget das gesamte Netzwerk übernehmen kann? Die Zahl der vollwertigen Knoten, die prinzipiell in der Lage wären, Blocks anzufertigen, nimmt seit einiger Zeit kontinuierlich ab, da die einfachen Netzwerkteilnehmer realisieren, dass sie keine Chance mehr haben, beim Mining zum Zug zu kommen. Einmal in die Blockchain eingetragene Transaktionen können später nicht mehr storniert werden, da ja alle Transaktionsblöcke aufeinander aufbauen.

Freuen Sie sich also, wenn Ihnen jemand versehentlich ein paar Tausend Bitcoin zuweist. Im Gegensatz zu herkömmlichen Zahlungssystemen kann diese Überweisung bei genügend nachfolgenden Blöcken praktisch nicht mehr rückgängig gemacht werden.

Die Problematiken des Bitcoin-Systems

Das Bitcoin-System weist aus meiner Sicht folgende Problematiken auf:

- 1. Hoher Benutzeraufwand (Pseudonyme)
- 2. Ineffizienz im Durchsatz von Transaktionen
- 3. Verschwendung von Ressourcen
- 4. Langfristige Anreizproblematik und fehlende Versorgungssicherheit
- 5. Abwanderung zu alternativen Kryptowährungen
- 6. Fehlende Angebotssteuerung
- 7. Uneinigkeit der Bitcoin Community
- 8. Preisvolatilität
- 9. Sicherheitsmängel
- 10. Unreguliertheit
- 11. Ungenügende Verteilungsungerechtigkeit (Kettenbriefcharakter)

Ad 1. Hoher Benutzeraufwand und 2. Ineffizienz

Einer der größten Makel des Bitcoin-Systems ist die ineffiziente Abwicklung von Zahlungsvorgängen. Das zieht sich von der Transaktionsgenerierung, die eine Vielzahl von Pseudonymen, Wechselgeldadressen und Verschleierungstaktiken notwendig macht, bis hin zu einer seriellen Verbuchung ohne Stornomöglichkeit, die zudem durch künstliche Schwierigkeitsgrade extrem aufwendig gestaltet ist. Dieser grundsätzliche Mangel des Bitcoin-Systems liegt im Kern an der Absage an eine zentrale Verbuchungsinstanz, die sich auf die Abwicklung von Zahlungstransaktionen spezialisiert hat.

Die Dezentralität des Systems und die prinzipielle Möglichkeit, dass jeder Netzwerkteilnehmer Transaktionen verbuchen kann, bedingt eine künstliche Verzögerung der Verbuchungsvorgänge, um eindeutige und einheitliche Registereinträge in der Blockchain gewährleisten zu können. Gegenwärtig werden neue Blocks nur alle zehn Minuten erstellt. Das ist ungefähr dann auch die Wartezeit eines Netzwerkteilnehmers, der auf eine Zahlungseingangsbestätigung wartet. Zu lange für einen effizienten Einsatz im Einzelhandel.

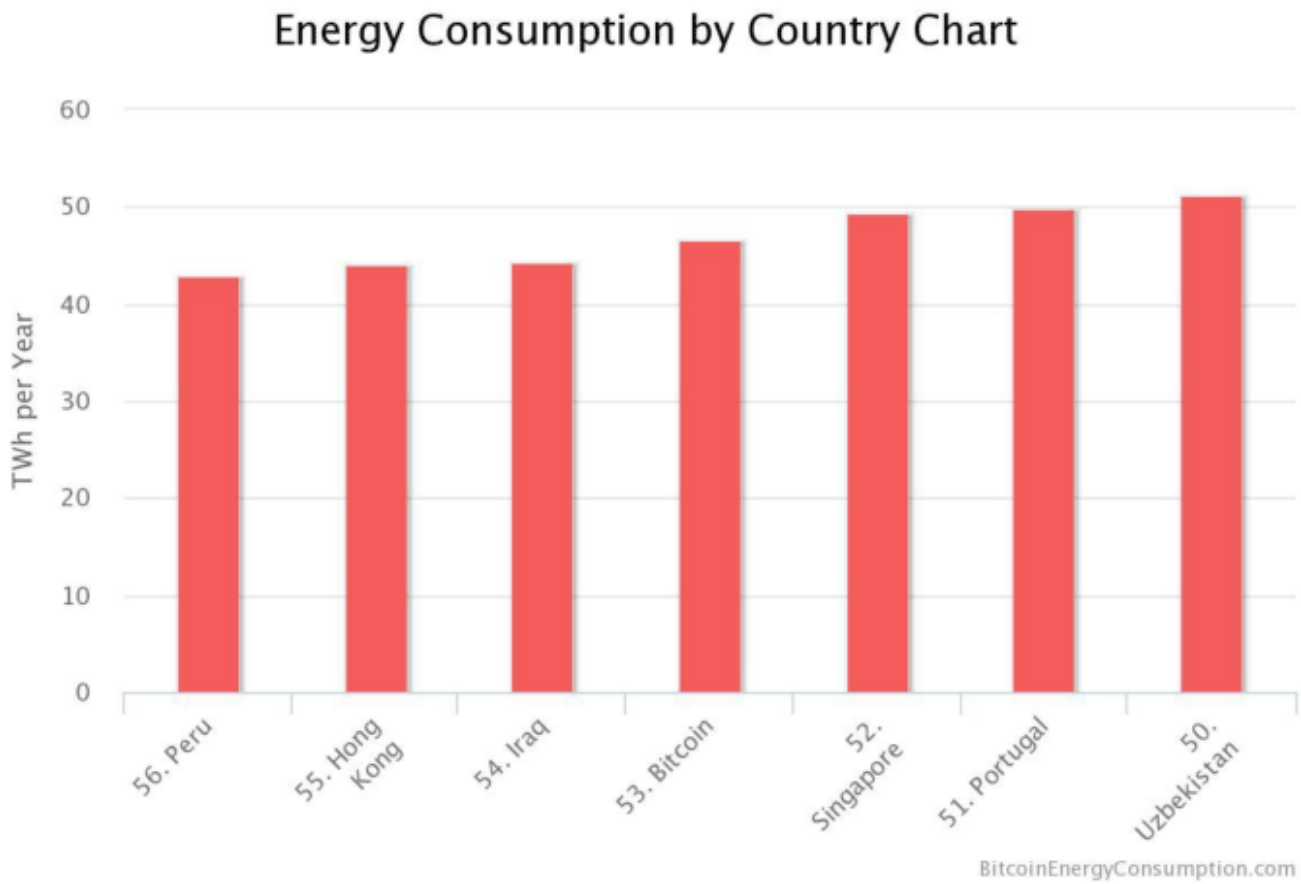
Bei der aktuellen Blockgröße ergibt sich ein Durchsatz von weniger als 10 Transaktionen pro Sekunde, während andere Zahlungssysteme in der Lage sind, viele Tausend Transaktionen pro Sekunde zu verbuchen. Auch potenzielle Verbesserungen wie eine größere Anzahl von Transaktionen pro Block oder Zahlungskanäle zur Verhinderung einer doppelten Verwendung des gleichen Guthabens (Double Spend), werden den Durchsatz des Bitcoin-Systems höchstwahrscheinlich nicht über ein paar zig Transaktionen pro Sekunde anheben können.

Ad 3. Verschwendung von Ressourcen

Noch schwerer ins Gewicht fällt jedoch die unnötige Verschwendung von IT- und Stromressourcen für das sogenannte Mining. Nach jüngsten Schätzungen des Bitcoin Energy Consumption Index von Digiconomist (1.2.2018) beträgt der hochgerechnete Stromverbrauch per annum mehr als 46 Terrawattstunden. Damit würde das Bitcoin-Netzwerk nahe annähernd so viel Strom verbrauchen wie die gesamte Volkswirtschaft Portugals. Mit dem Stromverbrauch einer Bitcoin-Transaktion ließe sich der Strombedarf von 17 US-Haushalten einen Tag lang decken.

Nun mögen die Zahlen etwas überzeichnet sein, da Digiconomist die Annahme trifft, dass die Kosten für die "Miner" immer 60% der Einnahmen betragen, was sich bei den extremen Aufwärtsschüben des Bitcoin-Preises in den vergangenen 18 Monaten nicht halten läßt. Aber es steht außer Zweifel, dass die installierte Rechenleistung im Bitcoin-Netzwerk stark zunimmt. Exemplarisch dafür mag einer der neuen Computerparks in der Inneren Mongolei stehen, der sich nur dem "Mining" von Kryptowährungen widmet.

21000 (in Worten: einundzwanzigtausend), auf Mining-Operationen spezialisierte Rechner sollen allein für die Schöpfung von Bitcoin installiert sein. Das Geschäft ist profitabel, nicht zuletzt deswegen, weil der Strom angeblich von lokalen Kohlekraftwerken subventioniert bezogen werden kann. Und das alles für die Verbuchung von ein paar Transaktionen, von denen ein guter Teil in anderen Zahlungssystemen unnötig wäre (Verschleierungs- und Wechselgeldtransaktionen). Gegen diesen Wahnsinn wirkt die Dot-Com-Blase der Jahrtausendwende ex post harmlos.



Quelle: Digiconomist.net, Stand 2.2.2018

Ad 4. Anreizproblematik und 5. Abwanderung zu alternativen Kryptowährungen

Was aber passiert, wenn die Vernunft wieder einkehrt? Wenn durch einen starken Preisverfall plötzlich Mining-Pools unrentabel werden? Wenn man aufhört, immer mehr Rechenleistung an ein ineffizientes Zahlungssystem zu verschwenden? Wenn die "Miner" realisieren, dass ein weiteres Hochrüsten der Rechenleistung nichts bringt, weil der Schwierigkeitsgrad für die Anfertigung eines neuen Blocks dann nach oben geschraubt wird? Die langfristige Anreizproblematik wird durch die Halbierung der Entlohnung nach einer bestimmten Blockanzahl noch verschärft.

Viele Mining-Pools werden dann entweder schließen oder sich alternativen Kryptowährungen zuwenden, die noch etwas mehr am Anfang stehen. Und diese, die sogenannten Altcoins, gibt es reichlich, da das Bitcoin-Netzwerk ja Architektur und Code weitgehend offengelegt hat. Wäre es da nicht sinnvoll, sich bei einem Kettenbrief etwas weiter vorne einzureihen? Da, wo der Schwierigkeitsgrad geringer und die Entlohnung noch größer ist?

Die einfachen Bitcoin-Nutzer sind dann in Gefahr, auf ihren Bitcoin sitzen zu bleiben. Sie sind darauf angewiesen, dass andere Netzwerkteilnehmer ihre Transaktionen verbuchen. Aber wer soll das machen, wenn alle Bitcoin schon emittiert sind. Prinzipiell kann zwar für jede Transaktion vom Sender ein zusätzliches Salär für den "Miner" in Aussicht gestellt werden. Aber es könnte dann trotz sinkender Schwierigkeitsgrade bei zurückgehendem Wettbewerb für die "Mining"-Seite zu wenig sein, um die aufwendige Blockgenerierung zu decken.

Diejenigen, die aus dem Bitcoin raus wollten, müßten dann das zusätzliche Salär für den "Miner" solange anheben, bis sich jemand für ihre Transaktion erbarmt. Schwarzmalerie? Man wird sehen. Aufgrund der limitierten Blockgröße gibt es für Transaktionen mit einem kleinen Gegenwert schon heute kaum Aussicht, einen Platz in einem Block zu ergattern, da die Transaktionsgebühr den Transaktionsgegenwert übersteigt.

Viele kleine Guthaben sind damit faktisch wertlos. In jedem Fall hat man die Abhängigkeit von einem Bankensystem mit definiertem Preis-Leistungs-Verzeichnis eingetauscht in die Abhängigkeit von einer anonymen Nutzergemeinde, die mit Sicherheit nicht nur aus Anthroposophen besteht. Von den Gefahren, die drohen, wenn der "Mining"-Wettbewerb so stark abnimmt, dass das gesamte Bitcoin-Netzwerk von einem Teilnehmer oder einer Teilnehmergruppe dominiert wird, (siehe 51%-Angriff) ganz zu schweigen.

Ad 6. Fehlende Angebotssteuerung und 7. Uneinigkeit der Bitcoin Community

Als ein Pluspunkt des Bitcoin-Netzwerks wird oft die Beschränkung des Geldangebots angeführt. Die Begrenzung auf 21 Millionen Bitcoin-Einheiten soll den Nutzern vermutlich Knappheit suggerieren. Die angebliche Knappheit dürfte aber kaum mehr sein als ein reiner Marketing-Gag. Die Halbierung der Bitcoin-Einheiten als Entlohnung für das "Mining" ist eine reine Willkür der Initiatoren des Systems. Niemand kann ihnen garantieren, dass es dabei bleibt. Aktuell ist die Beschränkung im Code implementiert, aber dieser könnte problemlos auch geändert werden, wenn sich die Bitcoin-Community darauf einigt. Aber wer ist das?

Welche Leitlinien bestimmen ihr Handeln und aus welchem Grund? Im Gegensatz zu Zentralbanken werden Sie auf diese Fragen kaum Antworten finden. Die Bitcoin Community besteht aus verschiedenen Interessensgruppen, die um die Deutungshoheit im Bitcoin-Netzwerk erbittert ringen. Neben der Gruppe, die sich der ursprünglich implementierten Bitcoin-Version verpflichtet fühlt (Bitcoin Core Entwickler), gibt es auch die "Miner" und Bitcoin-Börsen, die vor allem an hohen Gewinnen auf der Basis eines höheren Transaktionsdurchsatzes interessiert sind.

Im August 2017 spaltete sich die Bitcoin-Blockchain in zwei konkurrierende Äste auf: das herkömmliche Netzwerk und ein neuer Zweig, der sich Bitcoin Cash nennt. Beide Systemen basieren auf der gleichen Transaktionshistorie, das heißt die Blockchain ist bis zum Abspaltungszeitpunkt identisch. Bitcoin Cash hat den Anspruch, eine größere Anzahl von Transaktionen pro Zeiteinheit abwickeln zu können.

Einflußreiche Miner wechselten kurzzeitig die Seiten, wodurch es in beiden Netzwerken zu extremen Preisschwankungen kam. Die Zersplitterung des Bitcoin-Systems in alternative Systeme (sogenannte Hardforks) wird weitergehen, solange es für das Bitcoin-Netzwerk kein glaubwürdiges Gremium gibt, das die Regeln im Netzwerk begründet und festgelegt.

Eine willkürliche Begrenzung des Geldangebots ist aber auch aus anderen Gründen mehr als fragwürdig.

Die Hauptfunktion von (Bar)Geld ist es, dass es als wertbeständiges Tauschmittel und Recheneinheit zwischen den Wirtschafssubjekten zirkuliert. Der Teil des Geldeinkommens, der nicht für laufende Geldausgaben und zur Bestreitung des Lebensunterhalts gebraucht wird, wird bei klassischen Währungen Kreditsuchenden entweder direkt über die Kapitalmärkte oder indirekt über die Mittlerfunktion des Bankensystems zur Verfügung gestellt.

Das Bitcoin-System erfüllt beide Funktionen nur eingeschränkt bzw. gar nicht. Als Zahlungsmittel für Geldtransaktion ist es aufgrund eines ineffizienten Verbuchungsverfahrens und eben gerade auch wegen der künstlichen Angebotsbeschränkung, die sich in keinster Weise an der Nachfrage orientiert, nur in begrenztem Maße einsetzbar.

Eine Giralgeldfunktion in Form von Bitcoin-Kredit- und Kapitalmärkten gibt es ebenfalls nur in Ansätzen. Wenn eine Hauptmotivation hinter der Schaffung des Bitcoin-Systems der Gedanke gewesen ist, den Anspruch auf Zentralbankgeld (Giralgeld) durch eine direkte elektronische Geldeinheit zu ersetzen, die keine Forderung repräsentiert, dann wäre es widersinnig, Bitcoin-Kredite zu vergeben, die je nach Bonität des Kreditnehmers auszufallen drohen.

Nein, das Bitcoin-System ist nicht als Zahlungs- und Kreditmittel, sondern nach dem Vorbild von Gold als spekulatives Wertaufbewahrungsmittel gestaltet worden. Als eine jederzeit und von überall mobilisierbare Notfallreserve in Krisenzeiten. Aber im Gegensatz zu manchen Metallen sind Bitcoins nicht knapp. Sie müßten nicht mühsam geschürft werden. Im Gegensatz zu Gold können sie als Output eines Computerprogramms einfach und mit geringsten Kosten hergestellt werden.

Höhere Kosten fallen nur an, wenn aufgrund eines künstlich hohen Schwierigkeitsgrades ein ansonsten sinnfreier Rechenaufwand betrieben wird. Die künstlichen Schwierigkeiten sind ebenso wie das Versprechen einer Begrenzung des Bitcoin-Angebots reine Konventionen eines anonymen Netzwerkes, die jederzeit, wenngleich nicht ohne technische Schwierigkeiten, aufgehoben werden könnten. Im Gegensatz zu den Zentralbanken ist die Bitcoin-Nutzergemeinde nicht durch ein Gesetz verpflichtet, den Wert des Bitcoin zu erhalten.

Quelle: Thomson Reuters Datastream

Ad 8. Preisvolatilität

Auch als Recheneinheit eignet sich der Bitcoin nicht. Da der Bitcoin-Preis gegenüber gesetzlichen Zahlungsmitteln extrem schwankt, - eine tägliche Auf- oder Abwertung des Bitcoin zum US-Dollar im zweistelligen Prozentbereich ist keine Seltenheit - müssen Warenpreise in Bitcoin ständig angepaßt werden. Bei einem Bitcoin-Kurs von aktuell knapp 10.000 USD müssen kleine Preise mit vielen Dezimalstellen hinter dem Komma versehen werden. Der Bitcoin ist die schwankungsanfälligste aller Währungen.

Die auf Tageskursen berechnete Volatilität des Bitcoin-Kurses zum USD betrug seit Jahresanfang 2017 bis Anfang Februar 2018 41,6%, wobei die Volatilität bei einem so starken Trend vermutlich das falsche Maß ist, da sie lediglich auf Renditedifferenzen zum Renditemittelwert abstellt. Ein Wertpapier, das jeden Tag exakt um 10% stiege, hätte demnach eine Volatilität von Null Prozent. Aussagekräftiger ist in diesem Fall die prozentuale Differenz zwischen Hoch- und Tiefkurs über einen bestimmten Zeitraum. Seit Jahresbeginn 2017 sind das 2.332%, seit August 2011 sind es unfaßbare 845.461%.

Ad 9. Sicherheit

Kein Zahlungsmittel ist vollkommen fälschungs- oder einbruchssicher. Dennoch bieten elektronische Zahlungsmittel, die zudem zu einem Pseudonym transferiert werden können, für das nicht einmal eine Adresse hinterlegt werden muß, natürlich einen besonderen Anreiz für kriminelle Aktivitäten. Mit den wachsenden Online-Aktivitäten ist Ende der neunziger Jahre des vergangenen Jahrhunderts das Phishing aufgekommen. Mittels gefälschter Webseiten versuchen Hacker Nutzern Zugangsdaten zu entlocken, um Zahlungsmittel anschließend in Länder zu transferieren, in denen eine Strafverfolgung schwer möglich ist.

Große Hacker Communities existieren dem Vernehmen nach u.a. in Osteuropa, insbesondere in Rußland und Rumänien. Immer wieder wurden auch Bitcoin-Guthaben erfolgreich gehackt. Der spektakulärste Fall war der Zusammenbruch der japanischen Bitcoin Börse Mt. Gox. Im Februar 2014 stellte Mt. Gox einen Insolvenzantrag, nachdem 750.00 Bitcoin an Kundengeldern und 100.000 Bitcoin an eigenem Geld einfach "verschwunden" waren, angeblich durch einen Hacker-Angriff. Im März 2014 hatte Mt. Gox dann 200.000 Bitcoin "plötzlich wiederentdeckt".

Der Witz an der Geschichte ist, dass der Anspruch der Gläubiger gegen Mt. Gox von einem japanischen Gericht auf der Basis des Bitcoin-Kurses vom Februar 2014 mit einem Gegenwert von 413 Millionen USD festgestellt wurde. Die "wiedergefundenen" 200.000 Bitcoin wurden angeblich jedoch noch nicht verkauft und haben heute einen Gegenwert von ca. zwei Milliarden USD. Die Eigentümer von Mt. Gox könnten also trotz Pleite aus der Geschichte mit einem netten kleinen Profit herauskommen.

Ad 10. Unreguliertheit

Bis jetzt ist das Bitcoin-System noch weitgehend unreguliert. Während bei Waren- und Dienstleistungstransaktionen, die in einer klassischen Währung abgewickelt werden, fast überall auf der Welt Mehrwertsteuer abgeführt werden muß, ist diese Frage im Bitcoin-System meines Wissens ungeklärt. Was geklärt ist, ist der Punkt, welche Steuern fällig werden, wenn Bitcoins als Spekulationsobjekt gehalten werden. Auf Käufe oder Verkäufe von Bitcoin fallen analog zu Wertpapieren oder Devisen keine Mehrwertsteuer an. Gewinne aus solchen Transaktionen sind steuerfrei, sofern die Bitcoins länger als ein Jahr gehalten wurden.

Einkommen aus dem Bitcoin-"Mining" werden in Deutschland unter Gewerbeeinkünften erfaßt, die angefallenen Kosten (Strom, IT, Manpower) dürfen gegengerechnet werden. Unreguliert sind noch Kapitalbewegungen. Während es bei Bargeld eine Vielzahl von Meldepflichten und Geldwäschevorschriften gibt, genießt das Bitcoin-System hier noch Narrenfreiheit, was dem ein oder anderen Politiker schon sauer aufstößt. Das österreichische EZB-Ratsmitglied Ewald Nowotny wird im Januar 2018 in der Süddeutschen Zeitung mit den folgenden Worten zitiert:

"Es kann doch nicht sein, dass wir gerade beschlossen haben, den 500-Euro-Schein nicht mehr zu drucken, um Geldwäsche zu bekämpfen und jedem noch so kleinen Sparverein strenge Regeln aufbrummen, um dann zuzusehen, wie weltweit munter mit Bitcoin Geld gewaschen wird. Da besteht Handlungsbedarf".

Bezeichnend für die Zukunft des Bitcoin könnte das Ende von E-Gold gewesen sein. E-Gold war ein früher Vorläufer von Bitcoin, gegründet im Jahr 1996 und mit dem Beginn der Goldhausse ab dem Jahr 2000 schnell prosperierend. Das System war einfach aufgebaut. Die Teilnehmer eröffneten unter einem Pseudonym bei der Gold & Silver Reserve Inc. ein Goldkonto, auf das sie gesetzliche Zahlungsmittel einzahlten, die dann zum aktuellen Kurs in physisches Gold umgewandelt wurden. Warenkäufe, die mit E-Gold vorgenommen wurden, wurden in Bruchteilen einer Goldunze bezahlt. Die kleinste Einheit war ein

Zehntausendstel Gramm Gold.

Im Jahre 2004 sollen über eine Million Konten eröffnet gewesen sein und E-Gold war ein verbreitetes Zahlungsmittel im E-Commerce. Das Ende dieser vermeintlichen Erfolgsstory wurde durch einen regulativen Eingriff bewerkstelligt. Obwohl der Systembetreiber mit den Regulationsbehörden zusammenarbeitete und ihm noch im Januar 2006 vom US-Finanzministerium versichert wurde, dass für sein Geschäftsmodell keine Geldvermittlerlizenz gemäß dem USA Patriot Act vonnöten sei, klagten die US-Behörden in einer verschärften Anwendung des Gesetzes E-Gold (und später konkurrierende Systeme wie z.B. e-Bullion) gerade für das Fehlen dieser Geldvermittlerlizenz erfolgreich an.

Das zeigt, dass ein Staat wenig zimperlich sein- und im Zweifel auch auf den Rechtsgrundsatz nulla poena sine lege verzichten kann, wenn er vitale eigene Interessen bedroht sieht. Das Verfahren lief in den Jahren 2006 bis 2008 und es mag dazu beigetragen haben, das Bitcoin-System als dezentrales Netzwerk auszugestalten.

Ad 11. Verteilungsgerechtigkeit

Besonders viel zu verlieren haben die Benutzer der ersten Stunde, die mit dem Bitcoin-System bei gegenwärtigen Marktpreisen zu Millionären oder gar Milliardären geworden sind. Die Personen, die schon früh dabei waren und sich eine große Anzahl von Bitcoins verschaffen konnten, werden als Bitcoin-Wale bezeichnet. Eine direkte Zuordnung von Bitcoin-Einheiten zu Einzelpersonen ist nicht möglich, da ja, wie oben erläutert, Einzelpersonen eine Vielzahl von Pseudonymen (Bitcoin-Adressen) verwenden. Aber bereits eine Vermögenszuschreibung allein auf der Basis der Bitcoin-Adressen offenbart die extreme Ungleichverteilung des Bitcoin-Systems.

Eine Studie aus dem Jahr 2016 sah 20% aller zu diesem Zeitpunkt existierenden Bitcoin-Einheiten auf nur 115 Adressen verteilt. Der größte Bitcoin-Wal ist der Legende nach Satoshi Nakomoto - Sie erinnern sich, der Initiator des Bitcoin-Systems, dessen Identität nicht geklärt ist - mit einem vermuteten Vermögen von einer Million Bitcoin-Einheiten. Der aktuelle Gegenwert dieser Position ist knapp 10 Milliarden US-Dollar. Wenn Sie durch ein selbst ersonnenes Schneeballsystem in kurzer Zeit reich geworden sind, werden Sie vermutlich angestrengt darüber nachdenken, wie Sie wenigsten einen Teil dieses Reichtums in gesetzliche Zahlungsmittel oder andere Vermögensarten transformieren können.

Ein Direktverkauf der Bitcoin-Einheiten scheint ebenso absurd, als wolle Bill Gates seine Microsoft-Aktien alle auf einmal an der Börse verkaufen. Da das Bitcoin-System ein offenes Transaktionsregister ist, läßt sich für jeden Teilnehmer leicht nachvollziehen, wann die zuerst emittierten Bitcoin bewegt werden. Der Ausstieg der Insider der ersten Stunde hätte neben der fehlende Marktiefe und Liquidität noch eine verheerende psychologische Wirkung auf die Personen, die später eingestiegen sind. Die Folge wäre ein schneller Wertverfall in Richtung des inneren Werts der Bitcoin-Einheiten: der Null. Ihr virtuelles Bitcoin-Vermögen wäre wie Schnee in der Sonne zusammengeschmolzen, ohne dass Sie groß Stücke losgeworden wären.

Also muß ein anderer Weg her. Einer, der den neu in das System Eintretenden die Illusion beläßt, auch sie könnten mit dem Bitcoin noch reich werden. Am besten Sie bauen um den Bitcoin herum eine ganze Palette von Produkten, die den angeblichen Erfolg ihrer "Währung" signalisieren. Zum Beispiel einen laufend aktualisierten Bitcoin-Index, auf den strukturierte Produkte aufgelegt werden können. Einen Bitcoin-Future (tatsächlich sind es schon zwei Futures), der ihnen wenigstens teilweise ein Hedging ihrer Position ermöglicht oder gar Bitcoin basierte Wertpapier- und Kreditmärkte, die dem Ganzen den Anstrich geben, es handele sich beim Bitcoin um eine ganz normale "Währung", die einfach besser ist als alle anderen Währungen.

All dies lassen Sie von einem unkritischen Umgang der Medien mit dem Thema flankieren und heraus kommt im optimalen Fall eine Melange aus Überzeugungstätern und Spekulanten, die einen noch Dümmeren zur Realisierung ihrer Gewinne suchen (Bigger-Fool-Theorie). Aber wie sagte bereits ein österreichischer Pokerspieler treffend zu diesem Thema:

"Wenns Du den Dummen im Raum net erkennst, bist des am Ende selbst".

Was bleibt?

Um diese Frage zu beantworten, sollte zwischen dem Zahlungsmittel Bitcoin und der Blockchain-Technologie unterschieden werden. Nach den obigen Ausführungen ist kaum vorstellbar, dass der Bitcoin als Geldersatz eine große Zukunft vor sich hat. Die grundsätzliche Problematik des Zahlungsmittel Bitcoin lässt sich nicht lösen. Entweder der Bitcoin bleibt ein dezentrales Netzwerk prinzipiell gleichberechtigter Nutzer (Peer to Peer Netzwerk), das aufgrund vielfältiger Problematiken in der

Ausgestaltung eher früher als später in der Bedeutungslosigkeit verschwinden wird. Oder es hat den Anspruch sich als alternatives Zahlungssystem zu etablieren, das in Konkurrenz zu anderen Zahlungsdienstleistern wie VPay oder Visa steht.

In diesem Fall müssen große Effizienzsteigerungen im Transaktionsdurchsatz geleistet werden. Dies wiederum geht nur bei einem Verzicht auf Dezentralität und bei einer Spezialisierung einzelner großer Gruppen auf die Kernfunktion der Transaktionsverbuchung, die ohne künstliche Schwierigkeitsgrade und die Verschwendung von IT- und Energieressourcen auskommen muß. Für den Nutzer eines solchen Netzwerks stellt sich allerdings dann die Frage, welchen Vorteil er noch gegenüber den anderen etablierten Zahlungsdienstleistern hat.

Aber selbst wenn es dem Bitcoin-Netzwerk gelänge, hinsichtlich Kosten und Transaktionsdurchsatz konkurrenzfähig zu werden, bliebe das Verfahren der Neuemissionen von Bitcoin mehr als fragwürdig. Dass ein paar hochspezialisierte IT-Firmen die Seignorage, also die Differenz zwischen Herstellungswert und Gebrauchswert einer Währung, für einen im Kern einfachen Verbuchungsvorgang einsacken, läßt sich kaum rechtfertigen (auch nicht durch künstlich hochgetriebene Kosten der Bitcoin-Erstellung). Die Seignorage war schon immer ein beliebter Geldsegen für die Mächtigen dieser Welt. Jedes kleinste Fürstenhaus hatte im 18. Und 19. Jahrhundert sein eigenes Bargeld ausgegeben.

Selbst bei Goldmünzen ließ sich durch Münzverschlechterungen, das heißt durch eine Herabsetzung des Goldgehalts bei gleichbleibendem Nominalwert, noch ein Zusatzertrag erzielen. Kein Wunder, das mit dem Aufkommen der Nationalstaaten dieser Währungsvielfalt ein Ende gesetzt wurde, indem der Staat die Seignorage für sich beanspruchte und die Geldemission in Notenbanken zentralisierte. Das heutige Fiat-Geld kommt in die Welt, indem die Notenbank gegen Hereinnahme von überwiegend Staatsanleihen Zentralbankgeld ausgibt. Zuerst leiht sich der Staat für seine Ausgaben Kapital und danach kauft es eine andere staatliche Stelle wieder zurück, indem sie das Land mit einem Zahlungsmittel beglückt.

Damit die privaten Banken das schlucken, wurde ihnen durch Fractional Reserve Banking und Giralgeldschöpfung ebenfalls das Recht zur wundersamen Geldvermehrung eingeräumt. Ein derartiges System kann sich nur durchsetzen, indem die Menschen dazu gedrängt werden, dieses Geld auch zu benutzen. Dies wird bei gesetzlichen Zahlungsmitteln durch den Annahmezwang gewährleistet. Ein Privileg, das Bitcoin nie genießen wird, da kein Staat auf Seignorage verzichten mag.

Als Zahlungsmittel und Zahlungssystem wird der Bitcoin sich also nicht durchsetzen. Anders könnte das bei der zugrundeliegenden Verschlüsselungstechnologie aussehen. Die Blockchain ist nichts anderes als ein Register, in das unter bestimmten Regeln Informationen abgelegt werden. Die Kryptologie erlaubt allen Nutzern eine eindeutige Verifikation, von wem die Information zu welchem Zeitpunkt in einem Block abgelegt wurde.

Die Informationen sind in der Blockchain mit einem mathematischen Wert (Hashwert) verknüpft. Eine Manipulation oder eine Änderung der Daten ist nicht möglich, da sich dann andere Hashwerte ergeben würden. Das kling zunächst einmal ein wenig abstrakt. Aber die Blockchain-Technologie verfügt über den Vorzug, Nachweise darüber erbringen zu können, welche Informationen zu welchem Zeitpunkt existiert haben. Eine nachträgliche Datenmanipulation in der Art der sowjetischen Geschichtsschreibung oder die beliebte Ausrede des Nichtgewußthabens sind dann nicht mehr möglich.

Die Anwendungen der Technologie sind vielfältig. Ein Einsatz wäre zum Beispiel in Netzwerken denkbar, in denen ein 51% Angriff ausgeschlossen werden kann, da die Nutzer vertraglich dem gleichen Zweck verpflichtet sind und über die gleiche IT-Ausstattung verfügen. Also zum Beispiel in Firmennetzwerken, in denen buchhalterische Informationen wie z.B. Materialbestände verwaltet werden. Oder bei öffentlichen staatlichen Registern und bei Attesten oder Berufsabschlüssen, wo in einer Blockchain eindeutig verzeichnet ist, welche Dokumente ausgestellt wurden.

Gefälschte Dokumente wären wertlos, weil sie mit keinem Eintrag in einer Blockchain korrespondieren. Über die zweiteilige Signatur ließe sich zum Beispiel auch der Gebrauch von Gegenständen autorisieren. Mietautos könnten direkt starten, wenn der Benutzer mit einer kryptografischen Signatur nachweist, daß er die Berechtigung für dieses Fahrzeug hat. Die IT-Spezialisten, die heute ihr Geld noch mit der Programmierung von Bitcoin-Systemen zur Abwicklung von Finanztransaktionen verdingen, müssen also nicht (alle) auf dem "Müllhaufen der Geschichte" (Trotzki) landen. Wenn das mal kein versöhnliches Schlußwort ist.