Stand der Bitcoin Kritik heute

Erfasst am : 27. Juli 2022 00:04 | Erfasst von : Martin
Verknüpfte Kategorie(n): Beobachtungen, Bitcoin

Klare Ansage vorab: Ich verstehe Bitcoin, ich stehe 100% hinter den Konzeptionen von Bitcoin. Dennoch vergöttere ich Bitcoin nicht. Und in meinem Falle: mit Bitcoin meine ich immer die Kombination von Bitcoin als solides Fundament mit seinem ersten grossen, auf ihm basierenden Anwendungszweck: Schnelle Transaktionen = Lightning. Dazu etwas mehr später.

Ich möchte hier mal den Stand der aktuellen Bitcoin Kritik summieren und den gelisteten Punkten einen anderen Blickwinkel gegenüber stellen. Es möge mir gelingen. Sollte jemand mit mir in Dialog treten wollen, es gibt ja gleich nebenan das Kontaktformular.

Ich beginne mal mit der Summierung all der Absichten, die die Entwickler von Bitcoin hatten:

1. **Digitales Geld für eine zunehmend digitale, "kopierbare" Welt**
   Was so einfach klingt, ist in der Computerwelt extrem schwierig zu erreichen, denn ein Computer kann keine Materie bewegen, er kann aber Informationen kopieren. Nur sieht man dann einer Kopie nicht an, dass es eine ist - und dem Original nicht, dass es kopiert wurde. Und es will wohl keiner, dass digitales Geld von einem Hacker oder einem bösen Dämon einfach unbemerkt kopiert wird. Denn könnte man digitales Geld einfach duplizieren, wäre es kein Geld. Hierzu verweise ich immer gern auf das Buch Der Bitcoin Standard, denn welche Qualitäten ein Geld zu einem stabilen Geld machen, ist dort sehr anschaulich erklärt.

2. **Erlaubnisfreier Zugang**
   Jeder auf der Welt hat jederzeit vollwertigen Zugang zu BTC. Mit jede:r sind auch die gemeint, die keinen festen Wohnsitz haben, daher kein Bankkonto bekommen, und einfach üblicherweise mit einem Schulterzucken vom globalen Handel ausgeschlossen sind - weil uns reiche Länder deren Schicksal nicht oder nur wenig interessiert. Gerne mit dem Lokalitätsprinzip abgehandelt "nicht unser Problem, müssen die schon selbst richten". Ja, aber in Zeiten des Internets gibt es keine physische Geographie mehr.

   Der Afrikaner, der Vietnamese, der Albaner, der Tibeter, der Mandschure etc., Siedler und Nomaden, sind sofort und jederzeit mit ihren digitalen Leistungen erreichbar. Nur: Wie bezahlen? Bezahlen so, dass nicht Zwischenleute sich mit Wuchergebühren reich machen, sondern mein bezahlter Betrag zu 99.5+% beim Leistungserbringer ankommt?

3. **Dezentralität**
   Die zum Betrieb des Bitcoins nötige Infrastruktur ist derart, dass jeder, der einen kleinen Computer hat, daran teilnehmen und so die Infrastruktur-Basis bereitstellen und unabhängig machen kann. Je mehr das tun, desto dezentraler und manipulationssicherer. So dass es keinen Player mehr gebe, der sich irgendeine Monopolposition verschaffen kann. Weder Multimilliardär noch Schurkenstaaten, geführt von hoffentlich legitimierten, nur in sich selbst verliebten Egomanen. Ein solides Geld ist für alle ein Handelsmittel, kein Unterdrückungswerkzeug.

4. **Konsensregeln**

Alle Unklarheiten über Erschaffung von Bitcoins und deren Besitzverhältnisse werden innerhalb des Systems abschliessend und automatisiert gehandhabt. Es ist kein menschlicher Eingriff nötig.

5. **Nicht diskriminierend**
   Jeder, ohne Ansicht von Rasse, Glauben, Geschlecht, Gesellschaftsstatus, Ideologie, Landeszugehörigkeit, Alter, Genetik, Kaufkraft, Kenntnisstand etc. kann teilnehmen.

6. **Anonymität und Transparenz**
   Durch den Gebrauch von nur einmalig verwendeten Bitcoin-Transaktionsadressen sind zwar die Herkunft und der Werdegang seit "Geburt" eines Bitcoins unveränderbar nachvollziehbar, aber die hinter den Transaktionsadressen lebenden Besitzer sind mit den Mitteln des Bitcoin-Systems **nicht** eruierbar.

7. **Manipulationssicher**
   Niemand kann in der Erschaffung von Bitcoins jemand anderen auf Umwegen etc. übervorteilen. Es gelten für alle dieselben Regeln und derselbe Hüter: Die nicht vorhersehbare Ausgabe einer Hash-Funktion und die vom Konsens aller Teilnehmer akzeptierten Ansprüche an die Ausgabe, um als neu erschaffener Bitcoin gelten zu dürfen. Würde jemand den Konsens verlassen und hätte eigene Bitcoins, würde der Konsens den Gebrauch seiner Bitcoins automatisch ausschliessen. Damit ist die Motivation zum Beschiss gebrochen. Es ist lukrativer, im System nach dessen Regeln zu spielen, als dagegen. Das gilt sogar, wenn kriminelle Energie vorhanden ist: Der Bitcoin ist neutral, eine Bewertung seiner Nutzung ist eine menschliche und damit gefärbte, von aktueller Moral gefärbte Schubladisierung.

So, damit nun zu den Kritikpunkten:

1. **Vorwurf: Bitcoin ist eine Blase, Bubble**
   Eine Blase, ein Hype ergibt sich aus einem Impuls, dem viele aus mannigfaltigen Gründen folgen, ohne etwas oder nur viel zu wenig von der gehypten Sache zu verstehen. Das war bei der Dotcom Phase ums Jahr 2000 so wie auch bei der Finanzkrise 2008.

   Für Kenner der Sache ist sowas nicht neu, denn es gelten die Regeln des Schweinezyklus. Der heisst so, weil im frühen 20 Jahrhundert die Beobachtung gemacht wurde, wie sich Angebotsmangel (an Schweinen) mit hohen Preisen und Angebotsüberfluss mit billigen Preisen (und desaströsen Auswirkungen) auf die Agrarwirtschaft auswirkte.

   Gerade bei Bitcoin gab es dies bis zu ca. 2015 nicht. Bitcoin hatte also etwa sechs Jahre lang eine unbeschwerte Adoleszenz. Danach folgten sicherlich spekulative Einschüsse, weil Fiat-Geld ja im Überfluss in der Welt ist und angelegt werden will/muss. Dieser Fokuserhalt sorgte meiner Meinung nach garantiert zu Effekten des Schweinezyklus.

   Wenn nur aus dem Blickwinkel als Anlageobjekt betrachtet: Dies sollte der Bitcoin nie sein. Seine Kindheit beweist das ja auch. Er wurde erst zum Spekulationsobjekt wurde, als Investment-Sucher Geld auf den Bitcoin setzten - sicherlich unter vielen anderen gewinnversprechenden Assets. Eben der Gewinnmaximierung des Schweinezyklus folgend.

   Der in absolutem Wertvergleich wohl massivste Crash dann um 2017 zeigte, dass es auch damals noch keine substantielle und nachhaltige Nachfrage gab. In diesem Sinne reiht sich Bitcoin in viele andere Hypes ein - weder schlechter noch besser.

   Oder doch? Gute 25 Jahre (= eine Menschen-Generation) nach dem Internet wie es die

meisten kennen, dem HTTP, ist die jeweilige Fallhöhe immer grösser ... das heisst, dass die "Bubble" eben keine ist, denn wie auch das Internet überlebt die Konzeption des digitalen Geldes für die digitale Welt diese Rücksetzer. Das Internet ist hier. Punkt. Bitcoin ist hier. Punkt.

Gegenüber dem Internet hat der Bitcoin sogar noch den Vorteil: Man kann ihn einfach "stehenlassen". Würden Restriktionen von beliebiger Seite her den Zugang zu ihm blockieren ... die gespeicherte Transaktionsgeschichte bleibt auf allen Computern liegen. Und dass wir diese Maschinen in einem Wahn alle zerstören würden — daran glaubt wohl keiner auf der Welt. Bleiben Computer, bleibt das Internet, bleibt der Bitcoin.

Ob er eine Kauf- oder Tauschkraft haben wird in 10 Jahren, wie gross diese sein wird ... dies ist abhängig vom Bildungsstand der Menschen und was sie als wichtig oder wünschenswert erachten. Bitcoin braucht eine Community, eine Teilnehmerbasis. Denn wie alle menschengemachten Dinge: Menschen schaffen etwas, Menschen erhalten etwas. Ich hoffe im Förderlichen, dass es das Zahlungsmittel Bitcoin ist. Die Chancen stehen gut, aber wissen - kann man es nicht. Punkt.

2. **Vorwurf: Exorbitanter Stromverbrauch**
   Es ist schwer, die Annehmlichkeiten unserer modernen, westlichen Gesellschaften energiebilanztechnisch zu bewerten. Schliesslich hinterfragt wohl niemand mehr, ob es der Menschheit dient, dass

   - Elektrizität Licht ins Leben der Leute bringt und Fortschritt und Bildung ermöglicht
   - Klimaanlagen Hitze erträglich machen
   - TVs und Handys uns mit der Welt verbinden
   - Wäschetrockner einzelnen etwas Wartezeit abnehmen
   - eine moderne Küche ohne Stromverbraucher fast nicht mehr zu denken ist
   - Google und Wikipedia uns jederzeit unsere Fragen beantworten und Bildung bringen
   - Aluminium zu den leichtgewichtigen Werkstoffen gefertigt werden kann
   - Mobilität ein Schlüssel zu persönlicher Entfaltung in materieller wie auch immaterieller Sicht sein kann
   - in Zeiten des Klimawandels Wärmepumpen als Mittel der Wahl für Heizungen gelten
   - Öffentlicher, elektrischer Verkehr in den Städten uns mobil macht

   Was haben diese doch wohl vorwiegend anerkannt fortschrittlichen Dinge gemeinsam? Sie brauchen Infrastrukturen. Und diese sind nicht ohne. Wir wissen genau, dass diverse Infrastrukturen enorm ressourcenvernichtend, undemokratisch, ausbeuterisch, gesundheit- und umweltschädlich sind:

3. Da wir die Photovoltaik und die Energiespeicherforschung mehr als ein Jahrhundert lang einfach ignoriert, zumindest sehr vernachlässigt haben, weil es billiger war, weggespeicherte Sonnenenergie in Form von Öl und Gas wieder in die Atmosphäre zu holen, erzeugen wir die Premiumenergie mit Verbrennung. Und das, obwohl die gesamte auf die Erdoberfläche auftreffende Energiemenge der Sonne mehr als fünftausend Mal grösser als der derzeitige Energiebedarf der Menschheit ist.

   Ich sage jeweils: Die Technologie dieses Planeten ist die Photosynthese, der Energieaustausch via Zucker — alle Pflanzen und Tiere beherrschen diese Technologie, natürlich auch wir Menschen. Doch das Leben als Teil der Natur scheint dem Geist des Menschen nicht zu genügen, der Mensch will erschaffen ... und da er zwar seine Nachkommen mit der vorherrschenden Technologie erschaffen kann, aber eigentlich nicht genug über diese

Technologie der Natur weiss, stellt er ihr etwas gegenüber, was mit der nicht kompatibel ist: die unbelebte Technik. Und mit der zerstört er die Naturtechnologie, von der er selbst aber abhängig ist. Eigentlich nur zum Kopfschütteln ...

4. Enormer Naturverbrauch für Strassen, Individualverkehr, Energieverteilung. Wir geben soviel Natur hin, nur damit unsere Autos und Lastwagen drüberfahren können. Strassen erzeugen keinen Sauerstoff mehr, heizen sich auf, so dass man ohne Schuhe nicht mehr drauf gehen kann, und trennen Lebensräume. In Städten scheint man erstaunlicherweise erst jetzt festzustellen, dass Grünflächen die Hitze senken, Schatten spenden, Biodiversität steigern und den Wasserhaushalt regulieren. Ich persönlich ärgere mich regelmässig über die Kurzsichtigkeit, eine Fläche mit Beton versiegelt zu sehen, wo wir doch wissen, wie desaströs versiegelter Boden ist.

5. Schäden an Natur und Menschen durch Schadstoffe in der Luft, Abfall an den Strassenrändern, Abfall im Meer statt Recycling, keine Bildung bez. Umweltschutz und Recycling-Kreisläufe, Raubbau und Monokulturen, Ausbeutung von Völkern, Indigenen, kurzfristige Interessen Mächtiger wie Bolsonaro oder derzeit Putin, die sich einen Dreck um globale Wahrheiten scheren.

6. Schäden bei der Energiebeschaffung oder Abfallrecycling. Erdöl, seltene Erden, Gold, aber auch Nahrungsmitteln werden mit enormen Nebeneffekten ignoriert oder der Allgemeinheit überantwortet - zum Ziele wirtschaftlicher Gewinne. Atomare Abfälle zu entsorgen ist immer noch nicht gelöst.

7. Nicht zuletzt: Marode Infrastrukturen. Wenn elektrische Energie oder auch Lebensenergie, Wasser, einfach in veralteten, nicht anständig oder gar nicht gewarteten, nicht überwachten, abzweigbaren Transportsystem transferiert werden: Wie beim Wasser wird elektrische Energie ohnehin verschwendet, weil sie nur im Fluss was bewirken kann. Daher produziert man lieber mal zuviel, lässt sie dann auch ganz bewusst versickern, sich tot- oder wirkungslos auslaufen.

Aber eben, bei Vorwürfen an den Bitcoin blenden die meisten Kritiker einfach all das aus, was noch viel mehr Fokus verdiente. Man könnte derzeit eine Parallele ziehen zu den Ukraine-Flüchtlingen in Europa: Wie sehr sich doch alle um diese Kriegsflüchtlinge kümmer(t)en, wie leicht ihnen Zugang zu unseren Arbeitsplätzen, Sozialhilfen gemacht wurde - wo es doch beileibe nicht der einzige Krieg auf der Welt ist. Doch Krieg in Jemen, Syrien etc. bewog uns nicht zu gleicher Hilfsbereitschaft, im Gegenteil: Abschotten, Frontex, abschieben - Menschen sind schon irrationale Wesen ...

8. **Vorwurf: Elitäre Währung, Arme bleiben auch im Bitcoin-Standard arm**
   Ja, denn Bitcoin ist kein Weltretter. Wer jetzt Bitcoins hat und nicht veräussert, hat auch in Zukunft dieselbe Anzahl, denn es wird ja nicht mehr als die bekannten 21 Millionen geben. Wer sich jetzt einige Satoshis nur leisten kann, wird halt auch nicht mehr haben und es gibt keine Möglichkeit, passiv aus denen mehr zu machen. Doch wenn die Kauf- oder Tauschkraft des Bitcoin steigt, werden auch wenige Satoshis diese Steigerung mitmachen.

   Die Armut haben ja nicht Währungen gemacht, sondern die Politik, Religion, die Wirtschaft, die Globalisierung - sprich, die Gleichgültigkeit der Menschen in ihren Ländern. Der Bitcoin kann das nicht ändern, aber er kann dafür sorgen, dass ein Armer irgendwo auf der Welt am

globalen digitalen Wertaustausch mitmachen und seine Leistungsfähigkeit bezahlt anbieten kann. Denn das Handy, das gibt es mittlerweile ja schon überall auf der Welt.

Wer heute reich an Fiat ist, kann auch viele Bitcoins erwerben. Und wenn nicht kaufen, kann er sich zumindest das Mining überlegen. Auch hier hat er dann einen Vorteil, er kann sich mehr Apparate kaufen, die ihm eine statistisch grössere Treffermöglichkeit beim Mining verschaffen, aber eben keine Garantie, dass sich sein Einsatz vervielfache.

9. **Vorwurf: Volatilität**
   Aus Sicht der Gründer: wohl irrelevant. Das Spiel um Auf und Ab ist ja genau das Game der Fiat-Reichen und Mächtigen. Währungsmanipulationen sind gang und gäbe. Grossbanken sind fast alle verurteilt, weil sie sowas durchführ(t)en - egal in welchem Land. Bitcoin wie jedes andere Asset verliert ja nicht seinen innewohnenden Wert ... aber sein Tauschwert, der variiert halt ... das ist dann wieder der Schweinezyklus.

10. **Vorwurf: Keine materielle Grundlage**
    Seit Abkehr von Gold trifft das auf alle Fiat-Währungen zu. Dieser von den Mächtigen aus einer Verlegenheit der Mittelbeschafftung eingerichtete Beschluss war eigenmächtig, undemoktratisch und in höchsten Masse einfach eine Ignoranz bis dahin bestehender Anerkennung, wie Geld sein soll, um ein solides Geld zu sein. Aber mit solidem Geld konnte man halt nicht das machen, was die Mächtigen wollten.

    Doch unbesehen davon: Alles Geld ist ein Glaubenssystem. Wertpapiere auch. Gerade diese haben ganz offiziell den Status eines Glaubens, eines Hoffens, einer Wunschvorstellung, eines Vertrauens in Menschen, eine Idee. Denn keiner kann mit Geld etwas anfangen, wenn ein anderer es nicht will. Gold war für die Inkas auch nichts Spezielles. Die Gier der Invasoren danach brachte - neben unbekannten Krankheitserregern - den Untergang in ihre Gebiete.

    Auch für mich persönlich nicht - dürfte ich mir was Materielles herzaubern, wäre es sicher nicht Gold, auch nicht Platin, Diamanten oder was auch immer.

    Wertpapiere ... haben ihren Wert nur, weil sie eben eine Hoffnung verbriefen: Wäre ich ein Apple-Fanboy gewesen oder ein Musk-Jünger, ginge es meiner Depotbewertung schon besser ... aber eben, ich bin es nicht, ich gebe nicht meine durch Arbeit geminte Energie auf Luftschlösser weg. Im derzeitigen Fiat-System halt falsch gedacht. Natürlich finde auch ich Ideen von Musk interessant und wünsche ihren Durchbruch, man denke nur an seine Firmen Tesla, SpaceX und Hyperloop. Das sind wenigstens Fortschritte. Aber Apple, was soll an denen heute noch wertvoll sein? Was machen die für den allgemeinen Fortschritt der Menschheit?

11. **Vorwurf: Währung der Kriminellen, Dark Net**
    Tja ... wen wundert's dass Kriminelle, die ganz sicher anonym bleiben wollen, sich natürlich des Bitcoins als Transaktionsmittel bemächtigten. Schliess kann man in den überwachten Fiat-Geldflüssen ja eben nicht mal aus Kolumbien in die Schweiz über eine Bank ein paar Millionen überweisen. Da alarmieren die Bankenrechner sofort - und das von Staates wegen.

    Aber es ist dennoch zu kurz gedacht: Denn in der Blockchain ist Geburt und Werdegang eines Bitcoins von eben dieser, seiner Erschaffung aus lückenlos nachverfolgbar. Die dünne Schutzwand der Anonymität der Bitcoin-Adressen muss im Falle von Strafverfolgung halt die alten Tugenden durchdrungen werden: Folge dem Fluss des Geldes ... denn irgendwann wird ein anonymer Nutzniesser sich mit schwarzem Geld etwas Physisches leisten wollen. Ab dann

kommt digitale Kaufkraft in die physische Welt, wo wir leben. Auffällige Leute kann man hier ganz klassisch unter die Lupe nehmen.

In Fiat-Währung geht es viel leichter, Geldwäsche zu betreiben, egal, wie der Staat sie bekämpfen will. Wäre es anders, würden wir den Tatbestand der Geldwäsche ja nicht kennen.

Nun kann man sagen: eben, um diese Schattenwirtschaft zu bekämpfen, muss der Staat mit Geldflussüberwachung ja ankämpfen können. Jein, denn der Staat benutzt verknurrt dazu die Banken. Und er oder die Banken sind dann eben auch Zensoren. Und natürlich, echte Kriminelle brauchen ja nicht unbedingt eine Bank für ihre Geschäfte. Ihrer habhaft zu werden, klappt also nur bedingt.

Zudem habe ich erst letztens von einem IT-Forensiker erfahren, dass Bitcoin bei Drogenleuten immer noch recht beliebt ist – weil die Strafverfolgungsbehörden da nicht mehr so genau hinschauen oder nachkommen. Die menschlich sicherlich unisono verurteilte Pädophilie wird viel stärker verfolgt. Und was passiere? Diese Leute benutzen bevorzugt Monero, weil die vollständige Anonymität der Transaktionsdaten da ein Schlüsselmerkmal ist.

Die Rückseite dieser Sache ist aber, dass eben viele Leute kein Bankkonto haben dürfen, weil sie die Ansprüche der Überwachbarkeit nicht erfüllen - eben die Nomaden, die Armen, die Wohnungslosen, die Unregistrierten, die Unerlaubten ... sie zu opfern, nicht zuzulassen an Geldgeschäften, ist also der gesellschaftliche diskriminierende Preis, den Staat und wir eventuell für die Geldwäschebekämpfung zahlen. Und dass Staaten ihre Pappenheimer kennen und eventuell aus egoistische Gründen ja gar nicht so sehr am Austrocknen dieser Sümpfe interessiert sind, zeigen ja die laschen Massnahmen gegen Briefkastenfirmen auf Guernsey (GB) oder in Delaware (USA).

12. **Vorwurf: Eben gerade nicht so anonym wie Bargeld**
Bargeld ist nicht so anonym mehr. Ich hole mein Bargeld aus dem Bankomaten oder am Bankschalter. Dabei werde ich gefilmt. Natürlich nur zu meiner Sicherheit. Ohne Ironie. Aber wenn man nun denkt, das sei es auch: Nein, Banknoten können eine chemische Signatur im Bankomaten erhalten, die das mir ausgegebenen Geld mit mir verknüpft und verfolgbar machen, wenn diese Scheine wieder irgendwo auf ein geeignetes Prüfgerät treffen. Ein Bankomat kann heutzutage eine individuelle chemische Signatur aufs Papier bringen, die ein Mensch nicht erkennen kann. Fachleute haben da von bis zu drei chemischen Uhren gesprochen. Eine davon kann zur Umlaufszählung oder Bestimmung des Ausgabealters benutzt werden, die andere Reichweitenmessung, die letzte für Anbindung an mich als Bezüger des Scheins. Ein Bankomat könnte also auch einen Geldschein blockieren, vernichten, nicht akzeptieren ... der Fantasie sind bei Bargeld ebenfalls keine Grenzen mehr gesetzt.

13. **Vorwurf: Zu langsam, nicht geeignet für heutige Zahlungsflüsse**
Ja, dies ist wirklich ein Punkt. Die Gründe für diese vermeintliche Schwäche erläutere ich hier nicht weiter – sie lassen sich jedoch alle aus den eingangs erwähnten Absichten der Erschaffer ableiten. Nur soviel, seit ca. 5 Jahren ist auf dem Diamant-harten Buchhaltungsregister der Bitcoins, der Blockchain, die Lightning Technologie gewachsen, die zeigt, wie man schnelle und vor allem abgeschlossene Transfers rund um die Welt in Sekunden bei grösster Anonymität und Beschiss-Sicherheit und nach wie vor ohne notwendige menschliche Jurisdiktion durchführen kann.

Bei Lightning gilt nach wie vor das Bitcoin-Mantra: Don't trust, verify. Wenn eine Lightning Zahlung bei mir ankommt, kann niemand mehr sie blockieren, stornieren, zurückverlangen,

kein "Käuferschutz" eine Zahlung zurückhalten, keine Bonitätsprüfung die Zahlung verweigern. Wenn die Satoshis bei mir erscheinen, sind sie unverrückbar bei mir.

Man meine doch nicht, dass eine Visa- oder Mastercard-Zahlung Geld wirklich von meinem Bankkonto auf dasjenige eines anderen transferiert hat, wenn der Webshop mir anzeigt, dass meine Zahlung erfolgreich war. Es ist nur eine Aufzeichnung eines Bezahlungsversprechens, einer Transaktion, die wegen mangelnder End-zu-End Signaturen auch von den Beteiligten Infrastrukturbetreibern jederzeit manipuliert werden kann.

Weshalb wohl gibt es Trust-Programme von Visa oder MasterCard ... weil es eben Missbrauch gab und gibt. Was diese Firmen seit Jahrzehnten wissen und angesichts ihrer Gewinne getrost ignorieren können. Und erst in den letzten Jahren erkannt haben, dass das Vertrauen der Kundschaft geschmolzen ist. Also diese Marketing-Massnahmen von Trustprogrammen. Die nicht mal überall wirken: Mein Swisspass der SBB kann mir meine Kreditkarte ohne Benachrichtigung "belasten", obwohl ich verlangt habe, dass alle Belastungen meiner Kreditkarte gefälligst ein SMS auslösen sollen. Die damalige Erklärung seitens MasterCard: "Ja, wir haben dieses Programm, aber wir können unsere Partner ja nicht zwingen, es zu benutzen". Tja, ohne Worte. Bei Lightning geht sowas nicht.

14. **Vorwurf: Zu kompliziert für Otto Normalverbraucher**
    Das hat sicherlich gestimmt, je nach Wahl der Wallets gilt das wohl auch heute noch etwas. Wer sich allerdings beispielsweise auf dem Handy die Wallets Blue Wallet, Muun, Breeze oder Phoenix installiert hat, sieht, dass es mindestens so einfach ist wie bezahlen mit TWINT (CH). Einfach und schnell bei wesentlich grösserer Sicherheit als kontaktloses Visa, MasterCard oder was auch immer. Das Handy war für viele Ältere oder Technologie-Verweigerer anfangs auch undurchsichtiges Teufelszeug, Messengers wie WhatsApp, Signal oder Threema auch. Und doch, wenn mensch will, kann er/sie sich allem anpassen und damit umzugehen lernen.

15. **Vorwurf: Es gibt bessere Coins als Bitcoin**
    Nun, hierzu könnte ich die Technologie-Konzepte der Bitcoin-Gründer erläutern, aber Erklärvideos finden sich im Internet zu Tausenden. Nur ein Punkt will ich wirklich verstanden sehen: Der sogenannte Proof Of Work, ein Hallmark von Bitcoin. Er wird gerade im Zusammenhang mit dem Energieverbrauch immer kritisiert, es gäbe doch sicherlich effizientere Lösungen. Bei meinem ziemlich soliden Kenntnisstand über Technologien und Informatik: Nein.

    Wieso? Es ist nicht der Energieverbrauch, der das ursächliche Problem ist, er ist nur eine mögliche Konsequenz: Sondern der Aufwand, den Miner (freiwillig) betreiben, um Bitcoins zu finden / minen. Das Bitcoin-Rätsel ist mit Computer-Power zu bewältigen, aber auch mit Papier und Bleistift. Nur, wenn ich das Rätsel nicht mit Erfolg lösen kann, dann muss ich halt mehrfach probieren. Genau das lassen sich Miner viel Geld kosten, weil die Computer dieses Rätsel viele Milliarden-mal in einer Sekunde spielen können im Vergleich zu mir als Mensch. Mit diesem Nadel-im-Heuhaufen-Suchen wollen sie die Wahrscheinlichkeit zu ihren Gunsten beeinflussen. Mehr ist es nicht.

    Zu den gewaltigen Zahlen verfasste ich vor Jahren den Artikel Wofür also die Blockchain, der ein paar Berechnungen zum Zahlenraum präsentierte.

    Der Energieaufwand ist halt eine Auswirkung des Rätsels. Und daran zeigt sich auch: Es gibt offenbar keinen anderen Weg, das Rätsel zu knacken, als mit roher Rechenpower. Weder für Putin, USA, China, Musk, Amazon, Google, IBM, Quantenrechner ... die Hash-Funktion ist

die Magie für Integrity-Checks. Obwohl es theoretisch unendlich viele Lösungen gibt für einen bestimmten Hash, ist nur schon das Finden einer einzigen Lösung nur durch Versuch und Irrtum möglich. Nur darum ist der Energieverbrauch so hoch: Weil halt niemand weiss, wie er auf anderem Wege eine Lösung schneller finden könnte. Findet ein zweiter Leibniz, Einstein, Euler, Hawking etc. eine Lösung auf anderem Weg - Puff ist der Energieverbrauch weg. Aber dann auch die gesamte restliche, digitale Kommunikationsbasis, auf die wir ja kaum verzichten wollen oder können.

Das bedeutet im Umkehrschluss: Solange Proof Of Work der einzige Weg zur Erschaffung von Bitcoins ist, kann niemand bescheissen. Keine Regeln können ausgetrickst werden, keine geheimen oder diskriminierenden Absprachen getroffen werden, keine Machtverhältnisse betoniert werden. Das ist genau einer der Kronjuwelen am Bitcoin. Alle sind vor ihm gleich. Niemand ist gleicher. Niemand muss anderen trauen, die Hashfunktion ist der neutrale Richter. Alle anderen Regeln, Proof of Stake oder wie sie alle heissen ... haben genau das nicht ... es gibt den menschlichen Einfluss. Und der kann gebrochen werden. So ist es.

Die meisten alternativen Coins rühmen sich, dass es besser geht: Keine Limitation der Ausgabemenge, grössere Transaktionsblöcke, schnelleres oder "billigeres" Mining. Damit verwässern sie genau das, was Bitcoin eben diamanthart macht. Es bedarf halt der intensiven Beschäftigung, um zu erkennen, dass Bitcoin so sein muss wie er ist, um die eingangs erwähnten Ideen in der volatilen, digitalen Welt umzusetzen. Und nicht zuletzt: Der Bitcoin hat keine Wartungsmannschaft mehr, kein Aggressor kann Menschen real am Leben bedrohen, um seinen Willen durchzusetzen.

Aus aktuellem Anlass: Wieso lässt man Putin all seine Eskapaden durchgehen, sehend, dass es Tausende von Toten gibt? Weil der halt mit seinen Atombomben noch mehr Tote und eine lebensfeindliche Welt für alle hinterlassen kann. Der Starke muss mit den Idiotien von Schwachen halt etwas Geduld haben und andere Wege der Zurechtweisung finden. Wie in der Kindererziehung - Putin ist einfach ein Trotzkopf, der pubertierende Verhaltensmuster zeigt - das kommt am Ende ihres Lebens bei vielen vor, die zuvor nach ihren Ansprüchen nichts erreicht haben. Man könnte ihn mit Kriegsmitteln sanktionieren, aber das wäre eben noch schädlicher - für alle, für die Welt. Es ist schon schlimm genug, dass der Westen Fiat-Geld für Kriegsgeschäfte aufwirft, das eigentlich zur Anpassung an den Klimawandel hätte gesprochen werden sollen. Auf der anderen Seite: Jede Medaille hat eine Rückseite: Die dreckige Putin-Vorderseite und die erhellende Rückseite, dass einigen aufgeht: Die Energieversorgung muss wieder dezentral werden.

Wie auch immer: Man muss also abwägen, eben weil man real Menschen und das Leben bedroht sieht. Wie könnte man das bei Bitcoin machen? Es gibt niemanden (mehr), den man zur Änderung der Konsensus-Regeln zwingen könnte ... es hätte in den Jugendjahren des Bitcoin nur die sogenannte 51% Attacke gegeben ... aber das ist heute auch praktisch nicht mehr möglich, denn einer alleine kann nicht mehr das ganze Bitcoin-Netzwerk überzeugen, dass seine Blockchain die richtige ist ... angesichts der aktuellen Hashrate der Miner von ca. 220 Exa-Hashes pro Sekunde (22×10^{9}). Welcher Egomane könnte mit eigenen Resourcen diese Hashrate toppen? Und was dann erreichen? Wer das macht, würde ja im Bitcoin konform mitmachen wollen ... Niemand. Und damit erfüllt der Bitcoin eben eingangs erwähnte Designidee "Manipulationssicher".

Sollte ich ein Kriterium um den Bitcoin vergessen haben, freue ich mich, das zu erfahren. Ich würde gerne dann einen Pro- und Kontra-Punkt zu einem vergessenen Kriterium für mich selbst finden und

ggf. hier publizieren.

Fazit

Die Pandemie zeigte das Hauptproblem aller Währungen. Der Supply Shock. Unabhängig von irgendeinem Geld. Währung ist dazu da, ein Vertrauen in die Leistungsfähigkeit eines Handelsteilnehmers über ein Verwaltungssystem auf der einen Seite der Welt einem anderen Teilnehmer auf der anderen Seite verfügbar zu machen. Das Verwaltungssystem sind die internationalen und nationalen Banken. Ein Trustsystem ...

In Fiat-Geld müssen wir glauben, dass meine Bank irgendwie messen kann, ob der andere sein Geld wert ist. Die Banken sind also die heimlichen Eminenzen. Der Bitcoin will diese eliminieren. Das hat er aus meiner Sicht geschafft, denn er basiert nicht auf Einschätzungen irgendwelcher Leute, die eine Leistung Fiat-messbar machen wollen. Ich komme wieder auf Apple. Apple ist absolut überwertet. Apple macht nichts für die physische Welt. Hunderte anderer Firmen sind tiefer eingeschätzt, obwohl sie unendlich viel mehr physische Dinge in der Welt tun. Aber Apple ist ein Hype, drum ist deren Börsenwert so unverständlich hoch.

Solange alle physischen Bedürfnisse von uns allen gedeckt sind, können Fiat-Spieler machen was sie wollen. Nicht sie treiben den Zustand der Welt, sondern die Verteilung der physischen Güter, auf denen wir alle basieren. Das Bankensystem spielt das globale Spiel von Bewertungen und deren Verwaltung. Dummerweise bin ich als Arbeiter am Ende auch davon abhängig davon, denn die Zahl der CHFs am Ende eines Monats auf meinem Bankkonto ist die Bewertung, was ich für meine Lebenszeit bei Ansteller XY bekommen solle. Die Arbeiter sind die Ende der Glaubenskette, wir bekommen nur das, was die Banken uns zugestehen. Da wir alle aber in diesem System vernetzt sind, fällt uns deren Macht halt nicht mehr auf, denn auch der KMU-Gründer, der physische Dinger bewegt, ist dem Bewertungssystem ausgeliefert.

Und hier zeigt sich meine Hauptkritik an allen von Realitäten losgelösten Systemen, seien es Staatsanleihen, Derivaten oder Coins etc. Wir als Körper haben eine absolute Spielfeldgrenze, das ist das Umfeld, in dem wir leben, also die Erde. Unsere Körper können ohne sie nicht leben. Genauer, ohne all die Dinge, die unsere Körper halt ausmachen, die vom System Erde gefüllt werden können. Also, die Erde ist der Supplier, und bisher haben wir als moderne Menschheit noch keinen harten Supply Shock von ihr erlebt.

Die erwähnten losgelösten Systeme sind ein Bewertungssystem für diese physischen Dinge. Ein Bewertungssystem muss sich nicht um eigene Limiten kümmern, es muss ja nur das Physische bemessen. Wie die Mathematik: Man kann sie im Alltag sehr gut brauchen, aber Betrachtungen über eine Billion Nachkommastellen bei Pi ist mentale Spielerei für die, deren physische Bedürfnisse von der Erde gedeckt sind.

Der berühmte Spruch „Erst wenn der letzte Baum gerodet, der letzte Fluss vergiftet, der letzte Fisch gefangen ist, werdet ihr merken, dass man Geld nicht essen kann." sagt das doch an. Jeder physische Mensch muss dem zustimmen, denn ohne Nahrung innert zwei Monaten - eigener Tod. Das Ende der physischen Realität.

Die Pandemie ist ein kleiner Supply-Shock seitens unseres Lebensraumsystems. Wenn wir das begreifen, ALLE, dann werden Dekaden von Finanz-Produkt-Idiotien verschwinden, weil sie nichts Physisches tun. Die eingangs erwähnte Dotcom-Blase, die Finanzkrise ... ist jemand daran gestorben? Klar, beide haben Kummer verursacht, aber der Supply der Nahrungsmittel für die Menschheit war ja da.

Auch als das Container-Schiff Ever Given im Suez-Kanal quer lag, zeigte es uns, dass die physische Welt nach wie vor das Mass der Dinge ist, der Handel mit den physischen, lebensnotwendigen

Dingen. Was kam doch da alles ins Stocken ... eben ein Supply Shock.

Wäre es da nicht langsam sinnvoll, ein Bewertungssystem einzuführen, das eine Limite, eine harte hat und einer dem Lebensraum ähnlichen Realität nicht entfliehen kann? Eben, sowas wie Bitcoin?

Live long and prosper, Bitcoin.

PS: Wer englisch kann, sei eingeladen, diesen Podcast zu verstehen ... es war amüsant und vor allem dankenswert klar und direkt. Everything you know about the economy is wrong