Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 99 (2019)

Heft: 1066

Artikel: Der Geburtsfehler des Kryptogeldes

Autor: Birchler, Urs

DOI: https://doi.org/10.5169/seals-868667

Der Geburtsfehler des Kryptogeldes

Das Bitcoin-Protokoll ersetzt Vertrauen in eine zentrale geldpolitische Instanz durch einen Algorithmus. Das ist programmiertechnisch brillant, führt aber ökonomisch in die Sackgasse.

von Urs Birchler

«Papa, willst du Land auf dem Mond kaufen?» – «Wie bitte?» – «Land auf dem Mond. Gibt's im Internet.» Unser jüngerer Sohn (14), der mir das schmunzelnd offerierte, hat sein Angebot nicht aus der Luft gegriffen: Schon sieben Prozent der Mondoberfläche sind von selbstproklamierten Besitzern verkauft worden. Neu ist auch Mars zu haben. Oder Kryptowährungen. Wem nämlich ein «Blätz» auf dem Mond noch zu bodenständig ist, kauft Bitcoins oder einen der vielen anderen Coins und Tokens. Coinmarketcap.com sammelt aktuell über 2000 davon: Sie alle sind Einträge im Grundbuch des Nichts. Es ist, wie es der Digitalisierungsspezialist der finnischen Notenbank, Aleksi Grym, sagt: «Kryptowährungen sind Buchungssysteme für nichtexistente Anlagen.»[1]

Doch ist eine Papierwährung wie der Schweizer Franken nicht genauso fiktiv? Der innere Wert des Frankens ist seit der Loslösung vom Gold gleich null. Wir glauben an den Franken nur, weil alle anderen daran glauben, dass alle anderen an ihn glauben – eine reine Kollektivillusion. Die Schweizer Bauern des 19. Jahrhunderts begegneten den neu aufkommenden «Zetteln» genauso kritisch wie heute viele den Digitalwährungen. Mit der Zeit jedoch konnten sie sich mit Papiergeld anfreunden. Warum? Weil ein rechtlich-institutionell-politischer Unterbau entstand, der das Vertrauen in das von der Nationalbank ausgegebene Geld stützte. Vordergründig sind es die einzelnen Gesetze, die den Franken zum offiziellen Zahlungsmittel, auch für Steuern, machen oder die politische Unabhängigkeit der Nationalbank garantieren. Aber *deep*

«Wem ein ‹Blätz› auf dem Mond noch zu bodenständig ist, kauft Bitcoins oder einen der vielen anderen Coins und Tokens.»

Urs Birchler

Urs Birchler, zvg.

down ist es das gesellschaftlich-politische Grundgestein der Schweiz, auf dem unsere Papierwährung ruht: der Konsens über den Wert gesunder Staatsfinanzen und die Fähigkeit der Gesellschaft, Konflikte zu lösen, ohne die Notenpresse anzuwerfen. In anderen Worten: In unserem Papiergeld, dem Schweizer Franken, steckt Schweiz drin. In Bitcoin und den anderen Kryptowährungen steckt nichts.

Kann Bitcoin zur neuen Weltwährung werden?

Aber was, wenn Bitcoin trotz alledem die neue Weltwährung wird, wie es Apples Steve Wozniak und Twitter-Gründer Jack Dorsey prophezeiten? Was, wenn Bitcoin an die Stelle all der ausstehenden Dollars, Euros, Franken usw. tritt? Gemessen an der geschätzten Weltgeldmenge von rund 40 Billionen US-Dollar[2] wäre dann ein einziger Bitcoin, von denen es maximal 21 Millionen Stück geben kann, zwei Millionen US-Dollar wert – fünfhundertmal mehr als im April 2019.

Bitcoin entstand durch einen Geistesblitz von Satoshi Nakamoto[3], einer Vision des bis anhin Unmöglichen: der Kombination von digitalem und zugleich dezentralem Geld. Anders als Banknoten, die von einer Zentralbank ausgegeben und kontrolliert werden, und anders als unsere digitalen Bankguthaben, die auf einem zentralen Server der Bank abgelegt sind, liegen Bitcoins in Kopie auf den Computern sämtlicher Teilnehmer des Netzwerks. Digitales Geld hatte bisher das Problem, dass jeder Teilnehmer sich ohne entsprechende Kontrollen als jemand anders ausgeben oder das eigene Geld zweimal ausgeben, also Geld selbst «drucken» oder fälschen konnte. Die programmiertechnische Herkulesaufgabe war es daher, digitales Geld fälschungssicher und knapp zu halten. Denn was nicht knapp ist, taugt nicht als Geld. Aber alles Digitale (Folgen aus Einsen und Nullen), das einmal in der Öffentlichkeit ist, lässt sich perfekt und gratis beliebig oft kopieren. Und das Internet ist ein gigantischer Kopierer, dem kaum beizukommen ist: Musikindustrie und Zeitungsbranche haben das erfahren.

Knappheit und Vertrauen

Die Erfindung von Satoshi Nakamoto ist also die Schaffung von Knappheit in der digitalen Welt. Nakamoto erkannte das Potenzial einer damals schon fast zehn Jahre alten Idee mit dem prosaischen Namen «elektronischer Datumsstempel»[4]: Ein solcher Datumsstempel ermöglicht eine dezentrale Buchhaltung. Zahlungen werden chronologisch abgelegt und paketweise elektronisch versiegelt. Diese einzelnen Pakete oder «Blöcke» reihen sich zur berühmten Blockchain. Gibt nun jemand sein Geld zweimal aus, so gabelt sich die Kette der Zahlungen. Gültig bleibt dabei die längere der beiden Ketten, jene, an der die Ehrlichen weiterbauen – angenommen, die Ehrlichen sind in der Mehrheit.

Die Blockchain sichert, zusammen mit der maximalen Geldmenge von 21 Millionen Bitcoins (BTC), die Knappheit und Fälschungssicherheit von Bitcoin. Eher nebensächlich bei Bitcoin scheint der «Krypto»-Aspekt zu sein, der diesen Digitalwährungen den Namen gegeben hat. Es sind andere Kryptowährungen wie Monero oder ZCash, die einen stärkeren Fokus auf Privatsphäre, Anonymität, auf eine erhöhte Schwierigkeit der Nachverfolgung von Transaktionen setzen.

Die Maske einer privaten Geheimnummer mag die Attraktivität von Kryptowährungen für einzelne Teilnehmer erhöhen; zur tragenden Architektur gehört sie aus meiner Sicht nicht. Die Maskierung unterstreicht aber, dass das System dank eingebautem Identitätsmanagement ohne gegenseitige Kenntnis der einzelnen Teilnehmer auskommt, auch ohne Vertrauen in einzelne Partner, insbesondere auch ohne Vertrauen in eine zentrale Autorität wie eine Notenbank. Vertrauen – eines der knappsten Güter auf dieser Welt – wird also ersetzt durch einen Algorithmus: das Bitcoin-Protokoll. Diese Leistung ist programmiertechnisch brillant. Ökonomisch jedoch führt sie in die Sackgasse.

Bitcoin-Schürfer als Mitbuchhalter

Ein Student, nennen wir ihn Tobias, hat kürzlich eine Wohnung gefunden, «Strom und Heizung inklusive», schmunzelt er. Mit dem Gratisstrom speist er seine Geldmaschine: Er schürft Bitcoins.[5] Dazu muss man wissen, dass die Blockchain eine «Jekami-Buchhaltung» ist. Sie liegt in automatisch nachgeführten Kopien bei allen Teilnehmern des Netzwerks; diese verfügen über eine Art elektronische Kollektivprokura der Mehrheit. Als Teilnehmer am System ist Tobias daher auch Mitbuchhalter. Er hilft mit, Zahlungen in Bitcoin zu prüfen und abzusegnen. Seine Beteiligung (und diejenige vieler anderer) verhindert missbräuchliche Transaktionen einer Minderheit.

Zur Belohnung teilt ihm das System neue Bitcoins zu. Das System übersetzt jede Zahlung bzw. deren Überprüfung zunächst in eine anspruchsvolle Rechenaufgabe. Diese ist nur lösbar durch «Pröbeln». Doch ist das Resultat einmal gefunden, ist es einfach

In Kürze

Bitcoin ist eine verschwenderische Form von Stromgeld und somit eine Hightechversion von Primitivgeldformen wie Steingeld oder Muscheln.

Mit der Schaffung von Knappheit in der digitalen Welt verwirklicht Bitcoin einen programmiertechnischen Geistesblitz. Als alltagstaugliche Weltwährungen taugen Kryptowährungen jedoch nicht.

Wer Kryptogeld herstellt, erzeugt nichts. Diese Fantasiemünzen werden früher oder später von ihrer inneren Leere eingeholt. (rg)

zu kontrollieren.[6] Wer die Aufgabe zuerst löst, gewinnt («schürft») neue Bitcoins. Wer intensiver rechnet, also mehr Ressourcen beim *Mining* einsetzt, hat grössere Chancen, der oder die Erste zu sein; in dieser Lotterie entspricht der getätigte Rechenaufwand also der Anzahl der gekauften Lose.

Es ist der Stromverbrauch hinter der Buchprüfung, der indirekt sicherstellt, dass Bitcoins nicht missbräuchlich mehrfach verwendet werden können. Das Problem dabei: Mit zunehmender Rechenkapazität werden die Rechenaufgaben schwieriger; der Stromverbrauch steigt deshalb mit dem Erfolg des Systems. So verzehrte das Bitcoin-System auf dem bisherigen Höhepunkt des Bitcoin-Fiebers so viel Strom wie die gesamte Schweiz, also rund dreimal so viel, wie unsere Atomkraftwerke beisteuern.[7]

Bitcoin als Stromwährung

Bitcoin ist damit im Grunde eine Stromwährung. Übrigens nicht die erste: Schon 1932 schlug der Ökonom John Pease Norton einen mit Elektrizität gedeckten Dollar vor. Ein Spötter meinte, er würde der Regierung gerne anstatt Steuern 300 Volt schicken. Im Vergleich zu den Klimaeffekten einer Weltwährung Bitcoin klingt das noch fast harmlos. Der Stromverschleiss zeigt: Das Bitcoin-Protokoll schafft die Knappheit digitalen Geldes mit einem Trick. Es *erzeugt* keine Knappheit, sondern *importiert* diese bloss aus der realen Sphäre. Bitcoin als Stromgeld ist nur die Hightechversion der Primitivgeldformen wie Steingeld oder Muscheln – und eine verschwenderische dazu: Muscheln müssen nur einmal gesammelt werden. Die Bitcoin-Rechnerei ist bei jeder Verwendung bereits gewonnener Bitcoins erneut notwendig.[8]

So schürft am profitabelsten, wer den billigsten Strom hat. Tobias bezieht ihn von seinem Vermieter. Hacker benutzen via elektronische Hintertüren fremde Rechner. Grosse Bitcoin-Farmen stehen in alten Fabrikhallen im Glarnerland, in Island, in China. Oder in Venezuela, wo dank Hyperinflation die Währung und mit ihr der Strom zeitweise fast gratis waren. Ein Schweizer Start-up-Unternehmen plante den Bau von Containern voller Mining-Equipment: Mit Schiffen sollten sie jeweils an den Ort der billigsten Elektrizität gebracht werden. Parallel zur Jagd der Miner nach dem billigsten Strom haben die Computerhersteller auf das Mining von Bitcoin spezialisierte Chips erfunden, die in dieser Disziplin tausendmal schneller sind als unsere Feld-Wald-und-Wiesen-Rechner.

Bessere Rechner, billigerer Strom: Den Schürfern nützt alles nichts. Jede Kostensenkung lockt bloss neue Schürfer an – und zwar, bis die Gewinne für den marginalen Mitkonkurrenten wieder bei null sind. Es ist wie im Goldrausch: Reich werden ausser den Allerersten nicht die Goldgräber, sondern die Schaufelher-

«Ihre innere Leere wird diese Fantasiemünzen früher oder später einholen.»

Urs Birchler

steller. Die Kostensenkung führt zudem in eine Sackgasse. So führt Eric Budish von der University of Chicago an, dass zu billige Rechenkapazität das Bitcoin-System nicht wirtschaftlicher machen, sondern in seinen Grundfesten gefährden würde.[9] Wer nämlich, und sei es nur vorübergehend, 51 Prozent der Rechenkapazität kontrolliert, kann das System missbrauchen und beispielsweise eigene Bitcoins mehrfach ausgeben oder fremde Zahlungen sabotieren.

Das Bitcoin-Trilemma: Dezentralisierung, Sicherheit oder Kosteneffizienz

Ethereum-Mitbegründer Vitalik Buterin hat vorgeschlagen, die Belohnung der Teilnehmer anders zu berechnen. Statt aufgewendete *Rechenkapazität* (vergeudeter Strom) könnte der *Besitzanteil* der einzelnen Teilnehmer entscheiden. Nakamotos romantisch angehauchtes «eine Rechnereinheit – eine Stimme» würde ersetzt durch «ein Besitzanteil – eine Stimme». Der Unterschied erinnert an den Unterschied zwischen einer politischen Demokratie und einer Aktionärsdemokratie. Die Formel Besitzanteil statt Rechenaufwand hat einen einzigen grossen Vorteil: Der Energieaufwand wird eingedämmt. Dafür bringt sie andere Nachteile, vor allem Gefahren bezüglich Sicherheit. Diese Risiken wiederum könnte man zwar begrenzen, indem man wenigen ausgewählten Teilnehmern spezielle Rechte einräumt. So aber opfert man die Königin des Netzwerks, die Dezentralisierung.

Markus Brunnermeier (Princeton) hat das Design von Kryptowährungen deshalb als Trilemma dargestellt: Wir haben die Wahl zwischen Dezentralisierung, Sicherheit und Kosteneffizienz.[10] Alle drei sind nie gleichzeitig zu haben. Unser herkömmliches Zentralbankgeld ist einigermassen sicher (vor Fälschungen), sehr kosteneffizient (eine 1000er-Note kostet im Druck keine 50 Rappen), aber halt eben zentral organisiert. Bitcoin ist dezentral, ebenfalls ziemlich sicher, aber nicht kosteneffizient. Kosteneffizientere dezentrale Systeme sind möglich, aber nur mit Einbussen bei der Sicherheit. Heerscharen von Programmierern sind damit beschäftigt, in diesem Dreieck das Optimum zu suchen. Aber dem Dreieck entkommen werden sie nicht.

Das Grundproblem der Kryptowährungen liegt also nicht in erster Linie in ihren massiven Wertschwankungen, nicht in der Konzentration der Bitcoin-Rechner auf wenige «Mining-Pools», nicht darin, dass Bitcoins von Hackern gestohlen werden oder dass ein Börsenbetreiber sein Passwort und die damit geschützten Guthaben der Kunden mit ins Grab nimmt. Solche Symptome sind Ausdruck des Geburtsgebrechens der Kryptowährungen, des Brunnermeier-Trilemmas.

Besonders schlimm: Dieses Trilemma verschärft sich mit der Anzahl Teilnehmer am Bitcoin-System. Dezentralisierung bedeutet Duplikation bzw. Multiplikation des Rechen-, Kommunikations- und Speicheraufwands, der zum Identitätsmanagement notwendig ist.[11] Das Identitätsmanagement braucht auch Zeit[12], weshalb das Bitcoin-System mit zunehmendem Erfolg rasch enervierend langsam wurde – der Bezug einer Getränkeflasche am Automaten mit Bitcoin dauert eine ganze Stunde –, während der Stromverbrauch explodierte, lange bevor Bitcoin je einen nennenswerten Anteil am Weltzahlungsvolumen erreicht hätte.

Nie und nimmer wird Bitcoin zum Weltgeld

Tragischerweise ist die Blockchain deshalb für genau jene Anwendung denkbar ungeeignet, für die sie erfunden wurde: zur Verbuchung sehr häufiger Vorgänge unter einer grossen Zahl von Teilnehmern – kurz: für Zahlungsverkehr und Geld. Nakamotos programmiertechnisch geniale Verknüpfung von dezentralisierter Buchhaltung und Kryptogeld ist ökonomisch gesehen die perfekte *mésalliance*. Nie und nimmer wird Bitcoin oder einer seiner kleinen Brüder deshalb je zum Weltgeld.

Doch weshalb sind dennoch viele auf den Bitcoin-Zug aufgesprungen? Weshalb kaufen Investoren im Rahmen sogenannter Initial Coin Offerings (ICOs) irgendwelche Gutscheine, die meist nur durch vage, aber umso buntere Versprechen, ähnlich den Grundstücken auf dem Mond, gedeckt sind? Wie erreichte selbst ein Ablass von Sünden versprechender Jesus Coin (JC) vorübergehend eine Kapitalisierung von über 20 Millionen US-Dollar an den Kryptobörsen, bevor sich diese wieder in Luft auflöste? Die Antwort lautet: Eine spekulative Blase nährt eine Zeit lang sich selbst. Wer Angst hat, zu spät zu kommen, gibt den Vorgängern recht. Beim Kryptoboom kommt aber noch eine Illusion dazu: Die Bitcoin-Miner meinen, ihre geschürften Kryptoeinheiten seien den Verbrauch an Strom und Rechenkapazität wert. Ihre Kosten-

Nutzen-Rechnung scheint aufzugehen. Für die Gesellschaft jedoch geht sie nicht auf: Den Kosten der Kryptosysteme steht nichts Zählbares gegenüber. Das Schürfen von Gold fördert wenigstens ein Metall zutage, das auch als Schmuck Freude macht. Das Erzeugen von Kryptoeinheiten erzeugt nichts.

Eine spekulative Blase währt nicht ewig. Aber, wie Nobelpreisträger und bewährter «Bubble»-Warner Robert Shiller einräumt, wissen wir auch nie genau, wann eine Blase platzt. Spöttisch bemerkte er, auch Tulpen hätten immer noch einen positiven Preis; Bitcoin also könne auch in hundert Jahren noch existieren. Viele der anderen Kryptomünzen sind allerdings bereits klinisch tot. Als Faustregel gilt: Wenn eine Blockchain nicht wirtschaftlich ist ohne eine Ausgabe irgendwelcher Coins, lässt man besser die Hände davon. Klar, womöglich steht noch ein Dümmerer als Abnehmer da. Ihre innere Leere wird diese Fantasiemünzen aber früher oder später einholen.

Irgendwer ist dann der Letzte in der Kette – und der Dumme. Aber Vorsicht: Es erwischt auch die Gescheiten. Wer wegen Kryptospekulation zum Mond blickt, des Trabanten stille Bahn bestaunt und an die dort noch freien Grundstücke denkt, mag sich mit Isaac Newton trösten. Selbst Mitläufer und zuletzt Opfer der grossen Blase seiner Zeit, der Südseespekulation, klagte der grosse Physiker: «Ich kann die Bewegungen der Himmelskörper berechnen, nicht aber den Wahnsinn der Menschen.» Er hat nicht mehr erlebt, wie unsere schönen Algorithmen die Blockchain-Berechnungen erleichtern und gerade dadurch den Kryptowahnsinn unterstützen. ‹

[1]Aleksi Grym: The Great Illusion of Digital Currencies. In: Bank of Finland Economics Review 1/2018, https://helda.helsinki.fi/bof/bitstream/handle/123456789/15564/BoFER_1_2018.pdf
[2]Die Weltgeldmenge in breiter Definition liegt gemäss Berechnungen der CIA bei gut 80 Billionen US-Dollar (www.cia.gov/library/publications/the-world-factbook/rankorder/2215rank.html); rund die Hälfte davon, d.h. 40 Billionen, entfällt auf direkt zugängliches Geld, also Münzen, Banknoten und sofort verfügbare Guthaben auf Kontokorrents.
[3]Noch immer ist unbekannt, wer sich hinter diesem Pseudonym versteckt.
[4]Stuart Haber und W. Scott Stornetta: How to Time-stamp a Digital Document. In: J. Cryptology (1991) 3, S. 99.
[5]Durch das *Mining* (Schürfen) werden neue Blöcke erzeugt und zur Blockchain hinzugefügt.
[6]Ein vereinfachtes Beispiel: Welches sind die Primfaktoren von 4199? (13x17x19)
[7]www.strom.ch/de/energiewissen/stromverbrauch; https://digiconomist.net/bitcoin-energy-consumption
[8]Für den Hinweis danke ich Melanie Annaheim.
[9]Eric Budish: The Economic Limits of Bitcoin and the Blockchain. In: National Bureau of Economic Research Working Paper Series, No. 24717, Juni 2018.
[10]Markus K. Brunnermeier und Joseph Abadi: The Economics of Blockchains, 17. Juli 2018, https://voxeu.org/article/economics-blockchains
[11]Dies liegt auch an den sogenannten Latenzzeiten, dem Zeitverlust durch die Kommunikation zwischen den Rechnern.
[12]Aus Sicherheitsgründen erlaubt das System nur alle zehn Minuten einen neuen Block.

Urs Birchler
ist emeritierter Professor für Banking an der Universität Zürich. Er war viele Jahre Direktionsmitglied der Schweizerischen Nationalbank.

Zahl des Monats

anderes Leben nehmen, um danach das eigene ebenfalls von fremder Hand beenden zu lassen – das war gängige Praxis des Suizids im Europa um 1700. Vor allem im Gebiet des Heiligen Römischen Reiches, aber auch in Skandinavien und Frankreich war das (Selbst-)Morden zu beobachten. Es hatte zwei Gründe. Zuerst der religiöse: Selbstmord führt gläubige Christen auf direktem Weg in die Hölle. Wer lebensmüde und gleichzeitig Christ ist, hat also ein (weiteres) echtes Problem. Nun der weltliche: Die Obrigkeiten des 17. und 18. Jahrhunderts waren bei der Bestrafung von Kapitalverbrechen nicht zimperlich und setzten auf die abschreckende Wirkung der Todesstrafe. Gepaart mit den gängigen religiösen Überzeugungen hatte das Instrument aber die unbeabsichtigte Folge, dass Mord für die (gewiss kleine) Gruppe der Lebensmüden attraktiver wurde. Denn: Gläubige, die zum «mittelbaren Selbstmord» griffen, indem sie jemanden töteten, konnten vor ihrer Hinrichtung Busse tun und sich von ihren Sünden reinigen. Damit nun weder ihrer noch der armen Seele ihres Opfers der Weg ins Himmelreich verwehrt bliebe, töteten die Suizidalen vornehmlich kleine Kinder. Sie lesen richtig! Und die Erklärung dafür ist dann schon vergleichsweise rational: Kleinkinderseelen galten als rein und würden sich folglich ohne Probleme vor ihrem Schöpfer rechtfertigen können.
Erst im späten 18. Jahrhundert passten die Staaten ihre Rechtsprechung anreizkompatibel an: Wer tötete, um sich selbst richten zu lassen, wurde danach zu lebenslanger Haft bei Schwerstarbeit verurteilt und mitunter regelmässig öffentlich ausgepeitscht. Die Instrumente heutiger Staaten sind – meist – andere, aber das «Gesetz der unbeabsichtigten Folgen», das hier exemplarisch illustriert wird, existiert immer noch: etwa in der Geldpolitik, der Steuergesetzgebung oder der Bankenaufsicht. Falsch justierte Gesetze führen hier regelmässig zu unbeabsichtigten und unerwünschten Nebenwirkungen.

Alexander Fink ist Ökonom und arbeitet am Institut für Wirtschaftspolitik der Universität Leipzig und ist Senior Fellow am Institute for Research in Economic and Fiscal Issues – IREF.