Flossbach von Storch
RESEARCH INSTITUTE

WIRTSCHAFT & POLITIK 27/01/2025

Bitcoin, Altcoins oder Gold?

Für Privatanleger und für Zentralbanken? Oder für eine Geldreform?

von NORBERT F. TOFALL

Zusammenfassung

Bitcoin ist eine Fehlkonstruktion. Das spricht nicht gegen das ursprüngliche Konzept von Kryptowährungen. Sowohl Kryptowährungen als auch andere Privatwährungen können hilfreiche Mittel zur Entwicklung einer marktwirtschaftlichen Geldordnung sein.

Abstract

Bitcoin is a misconstruction. This does not speak against the original concept of cryptocurrencies. Both cryptocurrencies and other private currencies can be helpful tools for the development of a market-based monetary order.

Der Goldpreis ist im Jahr 2024 gemessen in US-Dollar um 27,22 Prozent und gemessen in Euro um 35,64 Prozent gestiegen. Der Bitcoin feiert historische Höchststände. Und der neue Meme-Coin von Donald Trump füllt die private Kasse des wiedergewählten Präsidenten der Vereinigten Staaten von Amerika.

Keine Woche nach Emittierung des „$Trump" unterzeichnet US-Präsident Donald Trump eine Executive Order, mit welcher die weitere staatliche Entwicklung von digitalem Zentralbankgeld verboten wird.[1] Gleichzeitig setzt er eine Regierungskommission ein, welche Vorschläge zur Stärkung privater digitaler Vermögenswerte sowie privater Kryptowährungen und Stablecoins zeitnah vorlegen und den Aufbau von Zentralbankreserven mit digitalen Vermögenswerten, wozu auch Bitcoin zählt, prüfen soll.

Ziel der Executive Order ist zudem die Förderung und der Schutz der Souveränität des US-Dollars, einschließlich aller Maßnahmen zur weltweiten Förderung der Entwicklung und des Wachstums rechtmäßiger und legitimer dollargestützter Stablecoins. Die Formulierung „promoting and protecting the sovereignty of the United States dollar" legt nahe, daß es Donald Trump nicht um eine Entnationalisierung des Geldes im Sinne von Friedrich August von Hayek geht,[2] sondern um das genaue Gegenteil, - allerdings in Verbindung mit ökonomischen Sonderinteressen des Silicon Valley und wohl auch seinen eigenen Geschäftsinteressen.

I.

Selbst Kritiker unseres derzeitigen Geldsystems – und der Autor dieses Beitrages zählt sich spätestens seit der Veröffentlichung des FAZ-Beitrages „Überwindung der Krise durch gutes Geld" im Jahr 2009 zu den Anhängern konkurrierender Privatwährungen im Sinne von Friedrich August von Hayek[3] – haben Zweifel, inwieweit die derzeitigen Kursentwicklungen von Bitcoin und Gold auf einen breiten gesellschaftlichen Vertrauensverlust in unser heutiges Geldsystem zurückzuführen sind oder inwieweit es sich um Folgen ökonomischer Problemverschleppungen in den westlichen Gesellschaften und um Reaktionen auf geopolitische Krisen und Gefahren handelt.[4]

Zwar können ökonomische Problemverschleppungen und geopolitische Krisen bei falscher geldpolitischer Weichenstellung zu einem gesellschaftlichen Vertrauensverlust in unser Geldsystem führen. Noch haben die falschen geldpolitischen Weichenstellungen in den westlichen Gesellschaften aber nicht zu einer

---

[1] Siehe Strengthening American Leadership in Digital Financial Technology – The White House

[2] Siehe FRIEDRICH A. VON HAYEK: *Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufmittel,* Tübingen (Mohr) 1977.

[3] Siehe THORSTEN POLLEIT, MICHAEL VON PROLLIUS, FRANK SCHÄFFLER und NORBERT F. TOFALL: „Überwindung der Krise durch gutes Geld", in: *Frankfurter Allgemeine Zeitung* vom 5. Juni 2009, Nr. 128, S. 12.

[4] Siehe auch A 'reverse conundrum' and foreign official demand for US Treasuries | CEPR

Vertrauenskrise in unser Geldsystem geführt. Es ist zwar eine Vertrauenskrise in unser politisches System und allgemein in die Geeignetheit unserer Politiker festzustellen. Unser Geldsystem wird in unseren westlichen Gesellschaften, obwohl es die tiefere Ursache vieler ökonomischer Problemverschleppungen darstellt, aber weder von den etablierten Parteien der Mitte noch von rechten und linken Populisten in Frage gestellt.

Im Gegenteil, während die etablierten Parteien der Mitte panisch am Status Quo festhalten, ist der Aufstieg rechter und linker Populisten ohne die politischen und ökonomischen Problemverschleppungen der letzten zwei Jahrzehnte nicht erklärbar. Es handelt sich um ihr Lebenselixier, ein Lebenselixier, das ihnen ausgerechnet von den etablierten Parteien stetig geliefert wird. Durch eine Geldsystemreform nach der unbereinigten Finanzkrise von 2007/2008 hätten sich diese Entwicklungen vielleicht verhindern oder zumindest einhegen lassen. Tempi passati…

Obwohl offen ist, wann durch zukünftige Finanzkrisen oder auch nur durch einen Börsencrash eine Vertrauenskrise in unser Geldsystem ausgelöst wird, stellt sich die Frage, welche Rolle Gold, Bitcoin oder alternative digitale Coins (Altcoins genannt) für eine Geldreform und neue geldpolitische Ordnungsformen spielen könnten. Zur Beantwortung dieser Frage ist ein kurzer historischer Rückblick sinnvoll und der Rückgriff auf ein fundamentales wirtschaftspolitisches Prinzip.

II.

„Alles spitzt sich (…) auf die Frage zu: Welche Ordnungsformen gewähren Freiheit? Welche begrenzen zugleich den Mißbrauch der Freiheitsrechte?“, betont Walter Eucken in seinen *Grundsätzen der Wirtschaftspolitik*.[5]

Der Mißbrauch der Geldordnung zur Durchsetzung politischer Macht ist so alt wie die Menschheit. Diese auf die Sicherung und den Ausbau politischer Herrschaft zielende Motivation steht letztlich hinter der gesamten Geldgeschichte, die sich als Geschichte der Geldmanipulationen lesen läßt.[6] Und auch der am Ende des Zweiten Weltkrieges in Bretton Woods vereinbarte Gold-Dollar-Standard und das darauf beruhende System fester Wechselkurse zum Dollar zerbrach, nachdem die US-Regierungen unter den Präsidenten Johnson und Nixon die Dollar-Druckerpresse auf Hochtouren laufen ließen, also monetäre Staatsfinanzierung im großen Stil betrieben. Dadurch wurde erstens Inflation in die Länder exportiert, deren Währung mit

---

[5] WALTER EUCKEN: *Grundsätze der Wirtschaftspolitik,* herausgegeben von Edith Eucken und K. Paul Hensel, 7. Auflage, Tübingen (Mohr/UTB) 2004, S. 179.

[6] Siehe PETER BERNHOLZ: *Monetary Regimes and Inflation. History, Economic and Political Relationships,* Cheltenham, UK (Edward Elgar) 2003, S. 1: „But it seems that especially rulers soon detected the potential to increase their revenues by tampering with its value. Already in antiquity we know ofmany cases of lowering the intrinsic metallic value of coins for this purpose. Examples are the minting of bad coins by Athens during the Peloponnesian War (Aristophanes, *The Frogs,*719-37) or by Rome during the Second Punic War, especially from 217 BC.”

dem Dollar in einem festen Wechselkursverhältnis verbunden war. Zweitens machten sich die Regierungen, die große Dollarbestände hielten, Sorgen um die Golddeckung des Dollar. Nachdem 1971 die französische Regierung unter Georges Pompidou ein Kriegsschiff nach New Jersey gesendet hatte, um Dollarreserven in Gold zu tauschen, und Großbritannien am 11. August 1971 diesem Beispiel folgte, verkündete US-Präsident Nixen am 15. August 1971 das Ende der Eintauschbarkeit des Dollar in Gold und damit das Ende von Bretton Woods.[7]

Sowohl das Ende des Bretton-Wood-Systems als auch die geldpolitischen Entwicklungen der 1920er und 30er Jahre führten Friedrich August von Hayek dazu, im September 1975 in seinem Vortrag „Choice in Currency" die Abschaffung des staatlichen Geldmonopols zu fordern.[8] In seiner Schrift „Entnationalisierung des Geldes" führt Hayek begründend aus: „Die bisherige Instabilität der Marktwirtschaft ist eine Folge davon, daß der wichtigste Regulator des Marktmechanismus, das Geld, seinerseits von der Regulierung durch den Marktprozeß ausgenommen wurde."[9] Und wenn „wir wollen, daß freies Unternehmertum und die Marktwirtschaft fortbestehen (...), haben wir keine andere Wahl, als das Geldmonopol der Regierung und nationale Währungssysteme durch freien Wettbewerb zwischen Emissionsbanken zu ersetzen."[10]

Staat und Politik muß die Macht über das Geld entzogen werden. Das führt nicht zur Anarchie, sondern zu einem anderen Ordnungsrahmen. Notwendig ist eine Geldordnung, eine Währungsverfassung, die als Ordnungsrahmen dem Primat von Recht und Freiheit zur Geltung verhilft. Das ist nur durch konsequente Machtteilung und nicht durch Machtkonzentration möglich.[11]

---

[7] Zu diesem und den nächsten Absätzen siehe NORBERT F. TOFALL: *Währungsverfassungsfragen sind Freiheitsfragen. Mit Kryptowährungen zu einer marktwirtschaftlichen Geldordnung,* Kommentar zu Wirtschaft und Politik des FLOSSBACH VON STORCH RESEARCH INSTITUTE vom 15. Januar 2018, S. 2-3.

[8] Vgl. HANS JÖRG HENNECKE: *Friedrich August von Hayek. Die Tradition der Freiheit,* Düsseldorf (Verlag Wirtschaft und Finanzen) 2000, S. 317.

[9] FRIEDRICH A. VON HAYEK: *Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufmittel,* Tübingen (Mohr) 1977, S. 94.

[10] Ebenda S. 127.

[11] Der europäische Sonderweg zu einer offenen Gesellschaft beruht auf der Machtteilung, auf Macht und Gegenmacht, siehe: HANS ALBERT: „Europa und die Zähmung der Herrschaft. Der europäische Sonderweg zu einer offenen Gesellschaft", in: DERS.: *Freiheit und Ordnung. Zwei Abhandlungen zum Problem einer offenen Gesellschaft,* Tübingen (Mohr) 1986, S. 9 – 59; STEPHEN HOLMES: „Differenzierung und Arbeitsteilung im Denken des Liberalismus", in: NIKLAS LUHMANN (Hrsg.): *Soziale Differenzierung. Zur Geschichte einer Idee,* Opladen (Westdeutscher Verlag) 1985, S. 9 – 41; MANCUR OLSON: *Macht und Wohlstand. Kommunistischen und kapitalistischen Diktaturen entwachsen,* übersetzt von Gerd Fleischmann, Tübingen (Mohr) 2002; ERIC L. JONES: *Das Wunder Europa. Umwelt, Wirtschaft und Geopolitik in der Geschichte Europas und Asiens,* 2. Deutsche Auflage, erweitert um das Nachwort zur 3. englischen Auflage, übersetzt von Monika Streissler, Tübingen (Mohr) 2012.

Und auch wer den Euro und die Europäische Währungsunion nachhaltig stabilisieren will, muß den Weg der konsequenten Machtteilung gehen und das staatliche Geldmonopol abschaffen, so daß dem Euro eine ihn stabilisierende Konkurrenz durch Privatwährungen erwachsen kann. Den EU-Regierungen und der EZB müssen die Möglichkeiten zur Manipulation des Geldes beschränkt werden und zwar durch Wettbewerb von konkurrierenden Privatwährungen.[12]

Staatliche Parallelwährungen sind zwar ein Schritt in die richtige Richtung von mehr Währungs- und damit mehr Systemwettbewerb, verlagern die Probleme von Machtmißbrauch und Geldmanipulation aber lediglich auf die nationale Ebene. Der Wettbewerb zwischen staatlichen Währungen ist erfahrungsgemäß nicht ausgeprägt genug, um staatliche Geld- und Zinsmanipulationen wirksam zu verhindern, was allein schon aus der Betrachtung der geldpolitischen Lage von Dollar, Yen und Euro und öfter zu beobachtenden weltweiten Abwertungswettläufen abgelesen werden kann. Zudem müssen wir uns wohl oder übel von der Vorstellung verabschieden, direkt oder über den Umweg einer staatlichen Parallelwährung zur alten Deutschen Bundesbank und ihrer Stabilitätspolitik zurückkehren zu können. Die 25 Jahre zwischen ca. 1973/74 und 1998/99, in denen die Bundesbank eine unabhängige, gegen die Machtinteressen der deutschen Regierungen gerichtete Stabilitätspolitik betrieben hat, sind die größte Ausnahme in der Geschichte der Geldpolitik und der Zentralbanken. Gemessen an der gesamten geldpolitischen Geschichte der Geldmanipulationen ist dies leider ein sehr kurzer Zeitraum.[13]

Echte dezentrale bürgerliche Gegenmacht, die *über nationale Grenzen hinweg* Recht und Freiheit und die Marktwirtschaft bewahren hilft und Geld- sowie Zinsmanipulationen weitestgehend verhindert, entsteht nur durch die Zulassung von konkurrierenden Privatwährungen. Die dezentrale millionenfache Nachfrage nach gutem Geld ist eine dezentrale bürgerliche Gegenmacht, die keine Regierung und keine EZB aufhalten kann, nachdem das staatliche Geldmonopol erst einmal abgeschafft oder aufgeweicht worden ist.[14]

III.

Die Aufweichung des staatlichen Geldmonopols hat durch die Entwicklung von Kryptowährungen kurz nach der Finanzkrise von 2007/2008 ihren Anfang genommen und entwickelt sich seitdem evolutionär weiter. Neben der Entwicklung von

---

[12] Vgl. FRANK SCHÄFFLER und NORBERT F. TOFALL: „Euro-Stabilität durch konkurriende Privatwährungen“, in: DIRK MEYER (Hg.): *Die Zukunft der Währungsunion. Chancen und Risiken des Euros,* mit Beiträgen von Helmut Schmidt, Václav Klaus, Arnulf Baring, Roland Vaubel, Wolf Schäfer, Hans-Olaf Henkel, Charles B. Blankart und anderen, Berlin (LIT) 2012, S. 275 – 288.

[13] Ebenda.

[14] Ebenda.

Kryptowährungen gab es seit 2008 aber auch vielfältige andere dezentrale private Initiativen, Privatwährungen zu entwickeln und zu emittieren.

Kryptowährungen sind ein Anwendungsfall von konkurrierenden Privatwährungen im Sinne von Friedrich August von Hayek. Da Kryptowährungen trotz des staatlichen Geldmonopols aufgrund ihrer dezentralen digitalen Konstruktion nicht so einfach zu verbieten sind bzw. ein Verbot nicht ohne weiteres durchsetzbar ist, kommt ihnen eine besonders relevante Rolle im Prozeß der Entstehung von dezentraler Gegenmacht zum staatlichen Geldmonopol zu.

Bereits Mitte der 70er Jahre unterbreitete Friedrich August von Hayek den folgenden Vorschlag:

„Der konkrete Vorschlag für die nahe Zukunft (...) besteht darin, daß sich die Länder des Gemeinsamen Marktes (möglichst einschließlich der neutralen Länder Europas, vielleicht später auch der Länder Nordamerikas) gegenseitig durch formalen Vertrag binden, weder dem Handel in ihren gegenseitigen Währungen (inklusive Goldmünzen) noch einer in gleicher Weise freien Ausübung von Bankgeschäften seitens jeder in einem ihrer Territorien gesetzlich niedergelassenen Bank irgendwelche Hindernisse in den Weg zu legen.“[15]

Durch Gewährung von vollständiger Produzenten- und Konsumentenfreiheit im Finanzsektor könnte es jedem einzelnen Bürger ermöglicht werden, zwischen staatlichem und anderem Geld zu wählen. Dazu müßte das staatliche Geldmonopol fallen und lediglich zugelassen werden, daß sich in dezentralen Entdeckungsverfahren parallel zum staatlichen Zahlungsmittel alternative Währungen, konkurrierende Privatwährungen, entwickeln können. Vorschriften bezüglich der materiellen Deckung von Währungen oder gar ein Goldstandard sind nach Ansicht von Friedrich August von Hayek sowohl unnötig als auch schädlich. Denn der „Wettbewerb würde sicherlich die emittierenden Institutionen weit wirksamer dazu zwingen, den Wert ihres Geldes (in bezug auf ein festgesetztes Güterbündel) konstant zu halten, als es irgendeine Verpflichtung zur Einlösung des Geldes in diese Güter (oder in Gold) könnte.“[16] Natürlich könnte es geschehen, daß sich bei freiem Wettbewerb zwischen verschiedenen Geldarten zunächst Gold als die beliebteste Geldart erweist. Die zunehmende Nachfrage nach Gold würde aber vermutlich zu einem solchen Anstieg und eventuell zu heftigen Schwankungen des Goldpreises führen, daß Gold aufhören würde, sich als Geldeinheit für den Geschäftsverkehr und das Rechnungswesen zu eignen.[17]

---

[15] FRIEDRICH A. VON HAYEK: *Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufmittel,* Tübingen (Mohr) 1977, S. 1.

[16] FRIEDRICH A. VON HAYEK: *Entnationalisierung ...* a.a.O., S. 32.

[17] Vgl. Ebenda, S. 102 und 127.

Inwieweit in einer marktwirtschaftlichen Geldordnung[18] gedeckte Währungen dominieren werden, läßt sich ex ante nicht bemessen, weil die einzelnen Menschen die freie Wahl haben, sowohl gedeckte als auch ungedeckte Währungen zu produzieren oder nachzufragen. Diese Währungen werden wie zur Zeit auch über Kredite oder durch Verkauf gegen andere Währungen verfügbar gemacht.

Die sofortige Zulassung von konkurrierenden Privatwährungen und eines allumfassenden Währungswettbewerbs wird jedoch nicht zu einem sofortigen vollständigen Verfall des staatlichen Geldes, zu einem „Rennen“ aus der Staatswährung und einem Zusammenbruch unseres gesamten Finanzsektors führen. Dieses wäre nur dann der Fall, wenn von heute auf morgen eine Situation vom Himmel fallen könnte, in der es ausreichend private Emissionsbanken und andere private Geldproduzenten gibt, die besseres als das staatliche Geld ohne Zeitverzögerung in ausreichender Menge und Verbreitung emittieren könnten, welches bei den Menschen zudem schon größeres Vertrauen erlangt haben müßte als die staatliche Währung. Um aus einer Währung sofort hinausgehen zu können, benötigt man auch sofort eine andere bessere Währung, in die man zu vertretbaren Kosten hineingehen kann.

Menschliches Handeln benötigt immer Zeit. Und aus diesem Grund fällt eine funktionierende marktwirtschaftliche Geldordnung auch dann nicht über Nacht vom Himmel, falls unsere derzeitige Geld- und Währungsordnung zusammenbrechen oder zumindest unter Druck geraten sollte. Auch eine marktwirtschaftliche Geldordnung kann sich nur schrittweise entwickeln.[19]

---

[18] Unter einer marktwirtschaftlichen Geldordnung wird eine wettbewerbliche Geldordnung verstanden oder genauer: ein reputationsbasiertes wettbewerbliches Geldsystem. Dieses unterscheidet sich vom Free Banking im engeren Sinne, das in der Regel auf dem Goldstandard basiert, durch die Zulassung unterscheidbarer Währungsstandards, siehe hierzu: PAUL TERRES: *Die Logik einer wettbewerblichen Geldordnung,* Tübingen (Mohr) 1999, S. 166 – 277.

[19] Das Problem, daß eine marktwirtschaftliche Geldordnung sich nur evolutionär entwickeln kann, wird leider sowohl von Ludwig von Mises als auch von seinem Schüler Murray N. Rothbard vollkommen unterschätzt. Dieses ist insofern erstaunlich, als eine der wichtigsten Theorieelemente der Österreichischen Schule der Nationalökonomie, durch die sie sich vom neoklassischen Gleichgewichtsdenken unterscheidet und welches Mises besonders betont hat, in der Einsicht besteht, daß menschliches Handeln Zeit benötigt und deshalb der Zeitlauf in theoretischen Modellen nicht vernachlässigt werden darf. Siehe hierzu: LUDWIG VON MISES: *Nationalökonomie. Theorie des Handelns und Wirtschaftens,* unveränderter Nachdruck der 1. Auflage, Genf 1940, München (Philosophia) 1980, S. 76 f. und JESÚS HUERTO DE SOTO: *Die Österreichische Schule der Nationalökonomie – Markt und unternehmerische Kreativität,* Wien (Hayek Institut) 2007, S. 62.

IV.

Obwohl es private Banken gibt, die in den letzten Jahren versucht haben, Finanzprodukte zu vermarkten, denen laut der Intention ihrer Produzenten eine Privatwährungsfunktion zuwachsen sollte,[20] entwickelt sich zur Zeit nicht aus diesen Versuchen eine relevante Gegenmacht für das staatliche Geldmonopol, sondern aus den Kryptowährungen. Das hat eine machtpolitische Ursache. Denn ein staatliches Verbot von Kryptowährungen ist nur sehr schwer durchsetzbar und wenn überhaupt dann nur in den Fällen, in denen die Konstruktion der jeweiligen Kryptowährung selbst Ansatzpunkte für die Durchsetzung eines Verbotes entstehen läßt.

Um das Phänomen Kryptowährungen zu verstehen und um dieses von anderen digitalen Währungen (wie digitales Zentralbankgeld oder die staatliche digitale Parallelwährung) abgrenzen zu können, sollte man sich klarmachen, daß Kryptowährungen die Mittel von Peer-to-Peer-Netzwerken sind, mit denen Menschen unter Ausschaltung von Vermittlern wie Zentralbanken und Geschäftsbanken Tauschhandlungen abwickeln können. Ideales Ziel dieser Peer-to-Peer-Netzwerke ist die dezentrale und direkte Kooperation zwischen Menschen, ohne daß Vermittler die Bedingungen dieser Kooperation manipulieren können. Im Idealfall sollen in diesen Peer-to-Peer-Netzwerken große Mengen von Transaktionen schnell, kostengünstig, transparent, sicher und anonym abgewickelt werden können.

Sehr vereinfacht formuliert setzt sich eine Kryptowährung – oder genauer: ein Kryptowährungs-Peer-to-Peer-Netzwerk – aus vier Elementen zusammen:

1. Distributed Ledger Technology oder Decentralized Ledger Protocol,
2. Konsensherstellungsmechanismus,
3. Authentifizierung und Anonymisierung der Nutzer mittels kryptographischer Verfahren und
4. Bezahlsystem mit eigener Währung.

Ein Distributed Ledger oder Decentralized Ledger Protocol ist ein dezentral verteiltes Kontobuch, in welches die Transaktionen des Peer-to-Peer-Netzwerkes eingetragen werden. Es handelt sich um eine Datei, die auf vielen Rechnern von Teilnehmern des Peer-to-Peer-Netzwerkes gespeichert ist, so daß bei einem destruktiven Zugriff auf einen Rechner oder bei staatlich oder sonst erzwungener Abschaltung dieses Rechners, das Kontobuch erhalten bleibt. Je breiter und globaler sich die Verteilung dieser Datei entwickelt, desto schwieriger wird es, das zugehörige Peer-to-Peer-Netzwerk lahmzulegen oder ein Verbot des gesamten Netzwerkes

[20] Siehe beispielsweise KARL REICHMUTH; REMY REICHMUTH: *Der RealUnit®. Zur Quelle der Geldwertstabilität,* Thun (Ott) 2001 sowie KARL REICHMUTH in Zusammenarbeit mit BEAT KAPPELER, JOACHIM STARBATTY und UWE WAGSCHAL: *Weg aus der Finanzkrise. Entscheid und Haftung wieder zusammenführen,* Zürich (Verlag NZZ) 2008. Der vom Luzerner Privatbankier Karl Reichmuth emittierte RealUnit ist dabei letztlich nichts anderes als ein Publikumsfonds.

durchzusetzen. Ein Distributed Ledger kann als Blockchain[21] organisiert werden, aber auch durch alternative Verfahren.[22]

Nun stellen sich die folgenden Fragen aus dem Bereich Clearing und Settlement:

- Wer darf was in das dezentral verteilte Kontobuch eintragen?
- Und wie wird sichergestellt, daß ein Eintrag in das dezentral verteilte Kontobuch wirklich eine Transaktion von Nutzern widerspiegelt? Wie wird der Konsens darüber hergestellt, bevor anschließend alle dezentral verteilten Dateien synchronisiert werden können?
- Und wie authentifizieren sich die Nutzer im Peer-to-Peer-Netzwerk? Und wer prüft das wie?
- Und wer bezahlt diejenigen, die das dezentral verteilte Kontobuch führen und die notwendigen Konsensprüfungen und Authentifizierungen durchführen?

Aus diesen Fragen ist unmittelbar einsichtig, daß es neben einem Distributed Ledger eines Konsensherstellungsmechanismus bedarf, der die einzelnen Transaktionen prüft und verifiziert, bevor sie in das dezentral verteilte Kontobuch des Peer-to-Peer-Netzwerkes eingetragen werden können. Sollte diese Prüfung und Verifizierung nur von einer zentralen Stelle durchgeführt werden, würde sofort ein entscheidender Ansatzpunkt erstens für Betrugsmöglichkeiten und zweitens für die Durchsetzung eines Verbotes eines Kryptowährungs-Peer-to-Peer-Netzes entstehen. Je mehr Rechner möglichst global verteilt an dieser Aufgabe beteiligt sind, desto schwieriger wird es, die Konsensherstellung zu manipulieren oder dieses notwendige Element zur Aufrechterhaltung des Peer-to-Peer-Netzwerkes außer Kraft zu setzen. Selbstredend gilt das auch für die Authentifizierung und Anonymisierung der Teilnehmer an diesem Netzwerk. Egal wie aufwendig durch Kryptographie (symmetrisch oder asymmetrisch) die Anonymisierung und Authentifizierung der einzelnen Nutzer erfolgt, wird diese Aufgabe von einer zentralen Stelle durchgeführt, so kann diese zentrale Stelle sehr viel einfacher manipuliert oder lahmgelegt werden als bei einem Prozeß, der von vielen global verteilten Rechnern durchgeführt wird.

Da es das Ziel von Peer-to-Peer-Netzwerken ist, die dezentrale und direkte Kooperation von Menschen zu ermöglichen, ohne daß Vermittler wie Zentralbanken und Geschäftsbanken die Bedingungen dieser Kooperation manipulieren können, benötigt ein Peer-to-Peer-Netzwerk ein Bezahlsystem mit eigener Währung als notwendiges Element, um diejenigen zu bezahlen, die den Distributed Ledger verwalten, die notwendigen Prüfungen und Konsensherstellungen und die Authentifizierung

---

[21] Siehe MELANIE SWAN: *Blockchain. Blueprint for a New Economy,* Cambridge et al. (O'Reilly) 2015.

[22] Siehe TONY ARCIERI: *On the dangers of a blockchain monoculture*, Blogbeitrag vom 5. Januar 2016, online unter: https://tonyarcieri.com/on-the-dangers-of-a-blockchain-monoculture

und Anonymisierung durchführen. Wird diese Währung von einer zentralen Stelle verwaltet, entsteht auch bezüglich dieses notwendigen Elements für Peer-to-Peer-Netzwerke ein Ansatzpunkt, das gesamte System zu manipulieren oder stillzulegen. Das wird umso schwieriger, je dezentraler und globaler dieser Mining- und Bezahlprozeß organisiert wird.

Aus der konkreten Ausgestaltung und Kombination der vier notwendigen Elemente eines Peer-to-Peer-Netzwerkes ergibt dann sich die Leistungsfähigkeit einer Kryptowährung hinsichtlich Transaktionsvolumen, Transaktionsgeschwindigkeit, Transaktionskosten, Transaktionssicherheit und Transaktionstransparenz.

V.

Wie die Entwicklung der heute bekanntesten Kryptowährung Bitcoin zeigt, ist Bitcoin gemessen an den Ideal-Zielen eines Peer-to-Peer-Netzwerkes leider eine Fehlkonstruktion. Sowohl die Organisation des Distributed Ledger von Bitcoin als auch der sehr aufwendige, immer komplexer und immer mehr Rechnerkapazität und Energiekosten verschlingende Prüf- und Konsensherstellungsprozeß von Bitcoin haben unter anderem dazu geführt, daß die Transaktionsgeschwindigkeit und das Transaktionsvolumen von Bitcoin gering und die Transaktionskosten sehr hoch sind. Diese strukturellen Probleme werden auch nicht durch das Lightning Netzwerk behoben. Das Lightning Netzwerk agiert letztlich nur wie ein Zahlungsdienstler an der Tankstelle, der in Vorleistung geht, während das Clearing und Settlement anschließend abgewickelt wird.

Die hohe Konzentration des Miningprozesse auf zu lokalisierernde Oligopole, der seine Ursache in der Ausgestaltung der ersten beiden Elemente dieses Peer-to-Peer-Netzwerkes hat, bietet auch viele Ansatzpunkte für staatliche Stellen, ein Verbot von Bitcoin durchzusetzen. Wenn ohne Ankündigung den Bitcoin-Minern der Strom abgestellt wird, ist zumindest fraglich, ob andere Miner diesen Kapazitätsausfall schnell ausgleichen können, um das gesamte Netzwerk aufrechtzuerhalten.

Diese und andere Probleme sprechen allerdings nicht gegen das gesamte Konzept von Kryptowährungen. Erste Versuche im Bereich neuer Technologien können nicht perfekt sein. Entscheidend ist, daß der Wettbewerb bessere Produkte hervorbringt. Mittlerweile sind über 10729 Kryptowährungen gelistet (Stand: 23. Januar 2025 um 16.00 Uhr),[23] die allerdings anhand der vier oben erläuterten Elemente zu untersuchen sind, ob es sich hierbei wirklich um Kryptowährungs-Peer-to-Peer-Netzwerke handelt oder lediglich um Digital Coins.

[23] Siehe www.coinmarketcap.com

Wenn es sich um Kryptowährungs-Peer-to-Peer-Netzwerke handelt, ist anschließend zu untersuchen, was in diesen Netzwerken konkret läuft und ob dort überhaupt etwas läuft. Werden die jeweiligen Peer-to-Peer-Instrumente überhaupt für Transaktionen genutzt oder sind sie reine Spekulationsobjekte oder Fun-Coins bzw. Shit-Coins? Oder Unterstützer- und Gedenk-Coins wie $Trump?

Die fast schon 17 Jahre umfassende Erfahrung mit der Kryptowährung Bitcoin zeigt, daß es die eine ideale Kryptowährung, die alle anderen Währungen verdrängen würde, letztlich nicht geben kann:

Ist die Verwaltung einer Kryptowährung strikt dezentral angelegt, sinkt die Transaktionsgeschwindigkeit und die Transaktionskosten steigen. Wird der Prüf- und Konsensherstellungsalgorithmus aus Sicherheitserwägungen immer komplexer und aufwendiger kann es zu Konzentrationen der „Prüfer“ kommen. Ist die Verwaltung dagegen zentral, kann die Zentrale das System manipulieren und ist anfällig für staatliche Eingriffe.

Die eine perfekte Kryptowährung läßt sich nicht mit einem Schlag konzipieren. Entscheidend ist deshalb, daß der „Währungswettbewerb als Evolutionsverfahren“[24] die Entwicklung immer besserer Kryptowährungen vorantreiben kann. Der Hauptnutzen der neuen Technologie für eine freie Gesellschaft und die Entwicklung einer marktwirtschaftlichen Geldordnung besteht nicht in der konstruktivistischen Konzeption der einen neuen idealen Währung, die angeblich in der Lage ist, unsere ökonomischen Probleme zu lösen. Der Hauptnutzen dieser neuen Technologie besteht für eine freie Gesellschaft darin, daß der Währungswettbewerb zwischen den Kryptowährungen, eine Vielzahl immer besserer unterschiedlicher Kryptowährungen für unterschiedliche Zwecke und Bedürfnisse hervorbringen kann und daß dieser Wettbewerb zwischen den Kryptowährungen über den Bereich dieser neuen Technologie hinaus auch heilsamen Wettbewerbsdruck sowohl auf andere Privatwährungen als auch auf die staatlichen Währungen ausüben dürfte.

Dabei dürften die eigentlichen Trial-and-Error-Prozesse noch vor uns liegen. Und daß die gesamte Technologie, welche Kryptowährungen überhaupt erst ermöglicht hat, die Geschäftsmodelle der bisherigen Vermittler der Finanzindustrie schon länger ins Wanken bringen, liegt auf der Hand. Aber auch Zentralbanken beobachten die gesamte Entwicklung sehr genau und beschäftigen sich mit digitalem Zentralbankgeld.

---

[24] Siehe Frank Schäffler und Norbert F. Tofall: „Währungswettbewerb als Evolutionsverfahren. Der Übergang vom staatlichen Papiergeldmonopol zu einer marktwirtschaftlichen Geldordnung ist evolutionär mittels Wettbewerb möglich“, in: Peter Altmiks (Hg.): *Im Schatten der Finanzkrise. Muss das staatliche Zentralbankwesen abgeschafft werden?,* München (Olzog) 2010, S. 135 – 155.

Technisch könnte sogar eine Situation entstehen, in welcher das gesamte heutige Bankensystem bei Überschuldung ohne Zusammenbruch des Zahlungsverkehrs abgewickelt werden kann, weil der Zahlungsverkehr, aber auch der Wertpapierhandel, schrittweise auf Peer-to-Peer-Transaktionen umgestellt wurde.

Und beachtet werden sollte auch, daß neben den idealen Reinformen von Kryptwährungs-Peer-to-Peer-Netzwerken auch Mischformen von Kryptowährungen mit anderen Privatwährungen nicht nur möglich sind, sondern gerade in dieser Kombination eine besondere Durchschlagskraft gewinnen könnten. So könnte man als Bezahlsystem anstelle einer ungedeckten Kryptowährung beispielsweise auch teil- oder vollgeckte Währungen verwenden. Eine beispielsweise vollständig mit physischem Gold gedeckte Währung hat gegenüber einer echten Kryptowährung zwar den Nachteil, daß man durch mögliche Beschlagnahme der Goldlagerstätte angreifbar ist, könnte für die Akzeptanz und die Verbreitung jedoch von Vorteil sein. Aber auch gut gemanagte Fonds könnten die Wertbasis für eine derartige Privatwährung bilden.

Ordnungspolitisch entsteht dadurch insgesamt eine Situation, in welcher dem staatlichen Geldmonopol zusehends Konkurrenz erwächst, was wirtschafts- und geldpolitisch eine enorme Relevanz gewinnt, falls Kryptowährungen aus welchen Gründen auch immer - vermutlich aber im Zuge einer der nächsten Finanzkrisen, wenn diese eine Vertrauenskrise in unser Geldsystem auslösen sollte - vermehrt von der breiten Masse als konkurrierende Privatwährungen genutzt werden könnten. Es ist deshalb nur zu hoffen, daß ein mögliches Platzen des Bitcoin-Hypes, nicht den gleichen Vertrauensverlust auslöst, wie einst das Platzen des Hypes um die Telekom-Aktie, welche die Lust der Deutschen auf die Aktie auf Jahre unterminiert hatte.[25]

VI.

Da Bitcoin gemessen an den Zielen eines Kryptowährungs-Peer-to-Peer-Netzwerkes eine Fehlkonstruktion ist, verwundert es nicht, daß Bitcoin heute keine nennenswerte gesellschaftliche Tausch- und Zahlungsfunktion erfüllt, sondern sich zu einem – allerdings hochriskanten – Mittel zur Wertaufbewahrung gewandelt hat. Ob angesichts der hochspekulativen Risiken überhaupt von einer Wertaufbewahrungsfunktion gesprochen werden sollte, ist umstritten. Auf jeden Fall sollten langfristige Anleger ihre Goldbestände im Portfolio nicht durch Bitcoin ersetzen, sondern ihr Bitcoin-Engagement aus der Spekulationskasse bestreiten. Allein die Möglichkeit, daß die Bitcoin-Miner aufgrund ihres Stromverbrauchs lokalisiert werden können und ihnen deshalb der Strom abgeschaltet werden kann (Greta Thunberg

[25] Siehe MARIUS KLEINHEYER: *Aktien für alle!,* Finanzsoziologische Analyse des FLOSSBACH VON STORCH RESEARCH INSTITUTE vom 15. Dezember 2017.

ist sicherlich dafür) und dann fraglich ist, ob andere Miner schnell und mit ausreichenden Kapazitäten in die Bresche springen können, sollte zur Vorsicht gemahnen.

Noch problematischer ist angesichts der Fehlkonstruktion von Bitcoin der Vorschlag, daß Zentralbanken eine Bitcoin-Zentralbankreserve aufbauen sollen. Einen ersten Vorschlag dazu gab es im US-Bundesstaat Texas,[26] welcher dann über die Big-Tech-Freunde von Donald Trump in die Öffentlichkeit getragen wurde und der jetzt auch Eingang die am 23. Januar 2025 unterzeichnete Executive Order von Donald Trump gefunden hat. Daß es im Interesse von Bitcoin-Besitzern ist, wenn Zentralbanken Bitcoin kaufen, was den Bitcoin-Kurs weiter nach oben treibt, liegt auf der Hand. Daß dadurch der ursprüngliche Zweck von Bitcoin, ein Peer-to-Peer-Netzwerk jenseits der Zentralbanken aufzubauen, konterkariert wird, ist offensichtlich. Mit einer „Entnationalisierung des Geldes“ im Sinne von Friedrich August von Hayek hat das nichts mehr zu tun.

Darüber hinaus stellt sich die Frage, wie eine Bitcoin-Zentralbankreserve ökonomisch begründet werden kann. Unter dem Goldstandard und im Bretton-Woods-System mit an den Dollar gekoppelten festen Wechselkursen war die Reservehaltung zur Vermeidung von Wechselkursanpassungen bei vorübergehenden Zahlungsbilanzungleichgewichten sinnvoll und nötig. Auch im System der floatenden Wechselkurse werden Reserven zur Glättung von Wechselkursschwankungen gehalten, um Störungen der Handelsströme zu vermeiden. Die Höhe dieser Reserven kann, was Thomas Mayer bereits 1980 in dem Beitrag „Exporterlösschwankungen und Investitionsgüterimporte“ ausgeführt hat, bestimmt werden als „Variabilität der Importkapazität und einer Politikvariablen, die die Reagilität der Importe auf Veränderungen der Importkapazität wiedergibt und damit den Trade-off zum Ausdruck bringt, der zwischen völliger Stabilisierung durch den Einsatz von Devisenreserven und maximalen Import besteht.“ Da Bitcoin als Transaktionsmittel so gut wie keine Rolle spielt und aufgrund seiner Fehlkonstruktion auch zukünftig nicht spielen dürfte, wird Bitcoin zur Glättung von Wechselkursschwankungen nicht benötigt.

Der Vorschlag aus den US-amerikanischen Big-Tech-Kreisen atmet deshalb den Verdacht, daß private Sonderinteressen durch den Staat bedient und damit die Geldordnung wie so oft in der Geschichte des Geldes mißbraucht werden könnte. Walter Eucken führte bereits in seinen Grundsätzen der Wirtschaftspolitik aus, daß die Freiheit auch dadurch bedroht sei, daß sich der Staat mit privaten Machtkörpern verbindet, was an den Untergang des römischen Reiches erinnere. „Unterschiede zwischen einst und heute bestehen; aber diese Unterschiede lassen die Gefahr nur noch größer erscheinen. Die Bevölkerung ist heute viel zahlreicher und lebt in größeren Massen zusammengeballt. Vor allem aber besteht heute ein industriell-

[26] Siehe https://capitol.texas.gov/tlodocs/89R/billtext/html/HB01598I.htm - Für diesen Hinweis danke ich meinem Kollegen Christof Schürmann.

technischer Apparat, der ein Beherrschungs- und Machtinstrument darstellt, das ältere Zeiten nicht kannten."[27]

Die heutige Verbindung von Big Tech und Big Government stellt ein Beherrschungs- und Machtinstrument dar, welches selbst Walter Eucken wohl nicht für möglich gehalten hätte. Und es besteht durchaus die Gefahr, daß die Möglichkeiten, welche Kryptowährungen und Altcoins zur evolutionären Entwicklung einer marktwirtschaftlichen Geldordnung bieten, durch diese Verbindung zielgerichtet gestört oder sogar zerstört werden. Sowohl Kryptowährungen als auch andere Privatwährungen können hilfreiche Mittel zur Entwicklung einer marktwirtschaftlichen Geldordnung sein, die Wohlstand für alle schafft. Sie können jedoch auch für Sonderinteressen mißbraucht werden, welche Wohlstand für alle behindern. Notwendig ist eine marktwirtschaftliche Geldordnung und nicht eine Verbindung von Big Tech und Big Government, welche die Geldpolitik und die Fed kapert.

[27] WALTER EUCKEN: *Grundsätze der Wirtschaftspolitik,* herausgegeben von Edith Eucken und K. Paul Hensel, 1952, 7. Auflage mit einem Gespräch zwischen Ernst-Joachim Mestmäcker und Walter Oswalt, Tübingen (Mohr Siebeck) 2004, S. 177-178.

RECHTLICHE HINWEISE

Die in diesem Dokument enthaltenen Informationen und zum Ausdruck gebrachten Meinungen geben die Einschätzungen des Verfassers zum Zeitpunkt der Veröffentlichung wieder und können sich jederzeit ohne vorherige Ankündigung ändern. Angaben zu in die Zukunft gerichteten Aussagen spiegeln die Ansicht und die Zukunftserwartung des Verfassers wider. Die Meinungen und Erwartungen können von Einschätzungen abweichen, die in anderen Dokumenten der Flossbach von Storch SE dargestellt werden. Die Beiträge werden nur zu Informationszwecken und ohne vertragliche oder sonstige Verpflichtung zur Verfügung gestellt. (Mit diesem Dokument wird kein Angebot zum Verkauf, Kauf oder zur Zeichnung von Wertpapieren oder sonstigen Titeln unterbreitet). Die enthaltenen Informationen und Einschätzungen stellen keine Anlageberatung oder sonstige Empfehlung dar. Eine Haftung für die Vollständigkeit, Aktualität und Richtigkeit der gemachten Angaben und Einschätzungen ist ausgeschlossen. **Die historische Entwicklung ist kein verlässlicher Indikator für die zukünftige Entwicklung.** Sämtliche Urheberrechte und sonstige Rechte, Titel und Ansprüche (einschließlich Copyrights, Marken, Patente und anderer Rechte an geistigem Eigentum sowie sonstiger Rechte) an, für und aus allen Informationen dieser Veröffentlichung unterliegen uneingeschränkt den jeweils gültigen Bestimmungen und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Sie erlangen keine Rechte an dem Inhalt. Das Copyright für veröffentlichte, von der Flossbach von Storch SE selbst erstellte Inhalte bleibt allein bei der Flossbach von Storch SE. Eine Vervielfältigung oder Verwendung solcher Inhalte, ganz oder in Teilen, ist ohne schriftliche Zustimmung der Flossbach von Storch SE nicht gestattet.

IMPRESSUM

Herausgeber Flossbach von Storch SE, Research Institute, Ottoplatz 1, 50679 Köln, Telefon +49. 221. 33 88-291, research@fvsag.com; *geschäftsführende Direktoren* Dr. Bert Flossbach, Dr. Tobias Schafföner, Dr. Till Schmidt, Marcus Stollenwerk; *Vorsitzender des Verwaltungsrats* Kurt von Storch*; Umsatzsteuer-ID* DE 200 075 205; *Handelsregister* HRB 120 796 (Amtsgericht Köln); *Zuständige Aufsichtsbehörde* Bundesanstalt für Finanzdienstleistungsaufsicht, Marie-Curie-Straße 24 – 28, 60439 Frankfurt / Graurheindorfer Str. 108, 53117 Bonn, www.bafin.de*; Autor* Norbert F. Tofall *Redaktionsschluss* 27. Januar 2025