Flossbach von Storch
RESEARCH INSTITUTE

WIRTSCHAFT & POLITIK 11/12/2020

Erneutes Interesse an Kryptowährungen

von NORBERT F. TOFALL

Zusammenfassung

Es ist fraglich, ob der Bitcoin die Vorherrschaft des US-Dollar brechen wird, wie die Financial Times in dieser Woche provozierend fragte.

Abstract

It is questionable whether bitcoin will break the dominance of the U.S. dollar, as the Financial Times provocatively asked this week.

I.

Als die Kryptowährung Bitcoin von Anfang Januar 2017 von ca. 1000 US-Dollar bis Dezember 2017 auf über 19 200 US-Dollar anstieg, schoß das Interesse für Kryptowährungen sowohl in ökonomischen Fachkreisen als auch in der allgemeinen Öffentlichkeit in die Höhe. Dieses Interesse schien jedoch weniger durch die ordnungspolitischen Reformmöglichkeiten von Privatwährungen[1] und einen möglicherweise entstehenden Währungswettbewerb zwischen Privat- und Staatsgeld motiviert zu sein, wie er in geldpolitischen Fachkreisen seit der Finanzkrise von 2008 diskutiert wurde,[2] als vielmehr durch die menschliche und legitime Neigung nach Gewinnstreben. Die Frage, ob eine lukrative Gewinnmöglichkeit bislang sträflich vernachlässigt wurde, war dominant. Das Interesse für Privat- und Kryptowährungen ebbte deshalb im Laufe des Jahres 2018 mit fallenden Bitcoin-Kursen wieder ab.

Wenig verwunderlich ist, daß die Aufmerksamkeit für Kryptwährungen im Jahr 2020 mit erneut steigenden Bitcoin-Kursen wieder gewachsen ist. Da diese Kurssteigerungen jedoch eindeutig auf die Corona-Krise und ihre schuldenfinanzierten staatlichen Bewältigungsversuche zurückzuführen sind, ist die dominante und in der Öffentlichkeit diskutierte Frage jedoch heute eine ordnungspolitische. Selten hat ein Bundesfinanzminister derart deutlich gefordert, daß man die Etablierung von privatem Geld verhindern müsse. Der Staat müsse sein Geldmonopol verteidigen. Und die *Financial Times* stellte in dieser Woche sogar die Frage, ob Bitcoin und digitales Geld die Vorherrschaft des US-Dollar beenden könnten.[3]

Angesichts der durch die Corona-Krise erzeugten neuen weltweiten Staatsschuldenhochstände, die selbst die *Financial Times* dazu veranlassen zu scheint, gewohnte Denkschablonen zu verlassen, muß in Erinnerung gerufen werden, daß die relevante ordnungspolitische Frage nicht die ist, die der

---

[1] Siehe Friedrich A. von Hayek: *Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufmittel,* Tübingen (Mohr) 1977, S. 94.

[2] 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 sowie 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 und 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.

[3] siehe: https://on.ft.com/33WAjZ1

deutsche Bundesfinanzminister Olaf Scholz formuliert hat. Denn die relevante ordnungspolitische Frage lautet nicht, wie der Staat mit allen nur erdenklichen Mitteln sein Geldmonopol verteidigen kann, sondern sie lautet nach Walter Euckens *Grundsätzen der Wirtschaftspolitik*: „Welche Ordnungsformen gewähren Freiheit?“[4]

Welche Geldordnungsformen gewähren Freiheit? Gemeint ist damit nicht mehr Handlungsfreiheit für Regierungen, sondern die Freiheit des einzelnen Bürgers. Es geht nicht um einen Primat der Politik, sondern um einen Primat von Recht und Freiheit.

Der Primat von Recht und Freiheit kann jedoch nur dann praktisch werden, wenn staatlichem Handeln - auch in der Geldpolitik - wirksame Grenzen gesetzt werden. Nur der Souverän eines freiheitlich-demokratischen Gemeinwesens, der Bürger, kann diese Grenzen setzen. Dabei geht es nicht um Anarchie und Anarcho-Kapitalismus, sondern um Macht und Gegenmacht im Sinne des katholischen Liberalen Lord Acton. Es geht um eine Ordnung der Freiheit. 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. Denn kein Mensch hält freiwillig schlechtes Geld. Und 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. 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.[5]

---

[4] WALTER EUCKEN: *Grundsätze der Wirtschaftspolitik*, herausgegeben von Edith Eucken und K. Paul Hensel, 5., unveränderte Auflage, Tübingen (Mohr) 1975, S. 179.

[5] Vgl. zu diesem und den folgenden Absätzen NORBERT F. TOFALL: *Währungsverfassungsfragen sind Freiheitsfragen. Mit Kryptowährungen zu einer marktwirtschaftlichen Geldordnung?* Studie zu Wirtschaft und Politik des FLOSSBACH VON STORCH RESEARCH INSTITUTE vom 15. Januar 2018, S. 7 – 10; online abrufbar unter:

https://www.flossbachvonstorch-researchinstitute.com/de/studien/waehrungsverfassungsfragen-sind-freiheitsfragen/

II.

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.

Um das Phänomen Kryptowährungen zu verstehen und um dieses von anderen digitalen Währungen (wie digitales Zentralbankgeld oder Stable Coins wie Libra, der jetzt Diem heißt) 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 durchzusetzen. Ein

Distributed Ledger kann als Blockchain[6] organisiert werden, aber auch durch alternative Verfahren.[7]

Nun stellen sich natürlich die folgenden Fragen aus dem Bereich Clearing und Settlement: Wer darf eigentlich 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 eigentlich diejenigen, die das dezentral verteilte Kontobuch führen und die notwendigen Konsensprüfungen und Authentifizierungen durchführen? Umsonst ist nur der Tod und nicht einmal der.

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 usw.) 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

---

[6] Siehe Melanie Swan: *Blockchain. Blueprint for a New Economy,* Cambridge et al. (O'Reilly) 2015.

[7] Siehe Tony Arcieri: *On the dangers of a blockchain monoculture*, Blogbeitrag vom 5. Januar 2016, online abrufbar unter:

https://tonyarcieri.com/on-the-dangers-of-a-blockchain-monoculture

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 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.

Wie die Entwicklung der heute bekanntesten Kryptowährung Bitcoin zeigt, weist Bitcoin gemessen an den Ideal-Zielen eines Peer-to-Peer-Netzwerkes leider erhebliche Mängel auf. 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. Die hohe Konzentration des Miningprozesse auf zu lokalisierende 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 in China der Strom abgestellt wird, ist zumindest fraglich, ob die Miner außerhalb Chinas 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 3900 Kryptowährungen gelistet (Stand Dezember 2020),[8] 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. Und wenn es sich um Kryptowährungs-Peer-to-Peer-Netzwerke handelt, dann ist zu untersuchen, was in diesen Netzwerken konkret läuft und ob dort

[8] Siehe www.coinmarketcap.com

überhaupt etwas läuft. Werden die jeweiligen Peer-to-Peer-Instrumente überhaupt für Transaktionen genutzt oder sind sie reine Spekulationsobjekte?

Die über 10 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“[9] 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.

Da niemand freiwillig schlechtes Geld hält, wird ein sich entwickelnder Währungswettbewerb alle privaten, aber auch die staatlichen Geldproduzenten dazu anhalten, besseres Geld zu produzieren. Die Produktion von schlechtem Geld – sei es Kryptogeld, anderes Privatgeld oder Staatsgeld – würde von den Menschen, wenn sie die freie Wahlmöglichkeit zwischen unterscheidbaren privaten und staatlichen Währungen haben, aufgrund ihrer Konsumentenfreiheit durch Abwanderung zu konkurrierendem Geld bestraft werden.

[9] Siehe Frank Schäffler und Norbert F. Tofall: „Währungswettbewerb als Evolutionsverfahren…“ a.a.O.

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 ins Wanken bringen, liegt auf der Hand. Aber auch Zentralbanken beobachten die gesamte Entwicklung sehr genau und beschäftigen sich mit digitalem Zentralbankgeld.[10]

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 der nächsten Finanzkrise, die eine Geldkrise sein dürfte - vermehrt von der breiten Masse als konkurrierende Privatwährungen genutzt werden könnten.

Fraglich ist jedoch, ob es die bekannteste aller Kryptowährungen, der Bitcoin, sein wird, der die Vorherrschaft des US-Dollar brechen wird, wie die Financial Times in dieser Woche provozierend fragte. Der Bitcoin weist aus den oben ausgeführten Gründen erhebliche Konstruktionsmängel auf. Denkbar und vermutlich wahrscheinlicher ist, daß in einer Situation, in welcher die Bürger das Vertrauen in staatliches Geld verlieren, ein Set unterschiedlicher Kryptowährungen den Staatswährungen wirksame Konkurrenz machen werden.

---

[10] Siehe NORBERT F. TOFALL: *Der digitale Renminbi als geopolitisches Mittel,* Kommentar zu Wirtschaft und Politik des FLOSSBACH VON STORCH RESEARCH INSTITUTE vom 17. November 2020 sowie NORBERT F. TOFALL: *Digitales Zentralbankgeld,* Kommentar zu Wirtschaft und Politik des FLOSSBACH VON STORCH RESEARCH INSTITUTE vom 14. Februar 2020.

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 AG 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 AG selbst erstellte Inhalte bleibt allein bei der Flossbach von Storch AG. Eine Vervielfältigung oder Verwendung solcher Inhalte, ganz oder in Teilen, ist ohne schriftliche Zustimmung der Flossbach von Storch AG nicht gestattet.

IMPRESSUM

Herausgeber Flossbach von Storch AG, Research Institute, Ottoplatz 1, 50679 Köln, Telefon +49. 221. 33 88-291, research@fvsag.com; *Vorstand* Dr. Bert Flossbach, Kurt von Storch, Dirk von Velsen*; Umsatzsteuer-ID* DE 200 075 205; *Handelsregister* HRB 30 768 (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* 11. Dezember 2020