

Daniel Leisegang

Demokratiefeindlicher Irrweg

Es sollte die Vision einer von Finanzinstitutionen und Nationalstaaten gänzlich unabhängigen Währung sein: Als Reaktion auf den Ausbruch der globalen Finanzkrise legte im Jahr 2008 ein Programmierer mit dem Pseudonym Satoshi Nakamoto (dessen wahre Identität bis heute ungeklärt ist) in einem wissenschaftlichen Papier den Grundstein für Bitcoins.¹

Umso überraschender ist es, dass nun ausgerechnet zahlreiche Staaten auf den Bitcoin-Zug aufspringen. In den USA sind Kryptowährungen als Zahlungsmittel wie auch als Wertanlage akzeptiert. Japan erlaubte Bitcoins im April dieses Jahres als legale Bezahlungsmöglichkeit im Einzelhandel. Und der russische Präsident Wladimir Putin versprach Anfang des Jahres ebenfalls, Kryptowährungen 2018 in Russland zuzulassen. Auch einige europäische sowie zahlreiche afrikanische Staaten fördern Bitcoins und andere Kryptowährungen gezielt.

Aus politischer Sicht ist dies eine verhängnisvolle Entwicklung. Denn dem Bitcoin-Netzwerk liegt eine anti-etatistische, mitunter sogar anarchokapitalistisch eingefärbte Ideologie zugrunde. Deren Anhänger verteufeln den Staat und streben nach einer Gesellschaft, in der Unternehmer und Eigentümer in einem „freien“ Markt nach Belieben schalten und walten dürfen – unbehelligt von Behörden und Regierungen.² Ausgerechnet Letztere scheinen jedoch allzu sehr vom Bitcoin-Hype geblendet zu sein, um dies zu erkennen. Hinzu kommt, dass sich die Utopie einer vermeintlich sicheren und demokratischeren Bitcoin-Welt längst in ihr Gegenteil verkehrt hat: Innerhalb des Netzwerks sind nicht nur die Vermögen hochgradig ungleich verteilt, sondern auch die Produktionsverhältnisse zunehmend vermachtet.

Code is law: Die Unsicherheit lauert im System

Die utopische Zuversicht der Bitcoin-Anhänger erwächst vor allem aus der hochkomplexen Netzwerk- und Datenbanktechnologie, auf der die Währung aufbaut: die Blockchain. Sie übernimmt die Funktion eines digitalen Kassenbuchs: In der Blockchain werden sämtliche Transaktionen verschlüsselt gespeichert; anschließend wird sie dezentral auf den Rechnern der Nutzerinnen und Nutzer hinterlegt. Anhand der Daten können diese dann jede

1 Vgl. Satoshi Nakamoto, Bitcoin: Ein elektronisches Peer-to-Peer-Bezahlsystem, www.bitcoin.de/de/bitcoin-whitepaper-deutsch-html.

2 Vgl. Ian Bogost, Cryptocurrency Might be a Path to Authoritarianism, www.theatlantic.com, Mai 2017.

einzelne Transaktion nachvollziehen, nicht aber deren Sender oder Empfänger identifizieren. Das ausgeklügelte Verfahren soll sicherstellen, dass die Bitcoin-Währung weder manipuliert noch gefälscht und auch nicht von Staaten blockiert werden kann.

Nicht die (Noten-)Banken, sondern die technischen Strukturen sollen also das Vertrauen in die Digitalwährung begründen.³ Dieses Versprechen ist jedoch überaus zweifelhaft. Denn in den vergangenen Jahren verloren zahlreiche Bitcoin-Nutzerinnen und -Nutzer Millionen an Euro – unter anderem, weil Cyberkriminelle Programmierfehler ausnutzten. So wurde im August 2016 die Bitcoin-Börse Bitfinex gehackt und um rund 58 Mio. Euro erleichtert. Bereits gut zwei Jahre zuvor – im Februar 2014 – vermeldete die in Tokio ansässige Handelsplattform Mt. Gox den Diebstahl von Bitcoins im Wert von damals 480 Mio. Euro. Als das Unternehmen kurz darauf Konkurs anmeldete, verloren die Nutzer ihr dort noch verbliebenes Geld endgültig.⁴

Derartige Diebstähle sind aus Sicht besonders ideologietreuer Bitcoin-Anhänger keine widerrechtliche Handlung. Die Grundidee der Kryptowährungen lautet, dass keine zusätzliche Übereinkunft und auch kein Gesetz die Regeln des Bitcoin-Handels bestimmt. Stattdessen bildet allein der geschriebene Programmiercode das vertraglich bindende Element – „Code is law!“, lautet die Devise.

Dass die Unsicherheit damit buchstäblich ins System eingeschrieben ist, zeigte sich anschaulich im Juni 2016, als das Kryptogeld-Projekt DAO gehackt wurde.⁵ Wegen eines Programmierfehlers konnte ein Angreifer auch hier einen Großteil des hinterlegten Kapitals auf eigene Konten abzweigen. Kurz nach der Tat tauchte ein Bekennerschreiben auf, in dem der mutmaßliche Hacker erklärte, lediglich die Möglichkeiten des Codes zu seinen Gunsten genutzt zu haben; etwas Unrechtes habe er somit nicht getan.⁶ Im Gegenteil: Das erbeutete Geld betrachte der Hacker als rechtmäßige Belohnung dafür, eine vorliegende Eigenschaft – ein „Feature“ – des Computercodes genutzt zu haben. Sollten die DAO-Betreiber ihm den Zugriff auf sein damit rechtmäßig erworbenes Geld verwehren, werde er juristisch dagegen vorgehen.⁷

Die Übermacht der chinesischen Miner

Selbst wenn es aber gelänge, sämtliche Programmierlücken in der Bitcoin-Software dauerhaft zu schließen, dürften sich die Anwenderinnen und Anwender nicht in Sicherheit wiegen. Denn das Bitcoin-Netzwerk ist von

3 Vgl. dazu den Beitrag von Rudolf Hickel in dieser Ausgabe.

4 Die Sicherung der Einlagen ist nicht vorgeschrieben, sondern bleibt dem Anbieter überlassen. Vgl. Bitcoin bei Cyberkriminellen beliebt – Schaden von 8,2 Mrd. Dollar, www.futurzone.de, 21.11.2017.

5 Die DAO („Dezentrale autonome Organisation“) sollte eine neue Form von Investmentgesellschaft bilden, die ausschließlich in Form von programmierten Verträgen (*Smart Contracts*) auf der Ethereum-Blockchain existiert. Vgl. Max Biederbeck, Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen, www.wired.com, 21.11.2016.

6 Vgl. www.pastebin.com/CcGUBgDG.

7 Dessen ungeachtet blieb ein Teil der Nutzer ihrer Überzeugung treu und lehnte jedes Sicherheitsupdate der Blockchain rigoros ab: Vgl. Axel Kannenberg, Nach dem DAO-Hack: Ethereum glückt der harte Fork, www.heise.de, 20.7.2016.

einer höchst ungleichen Verteilung der Ressourcen und den sich daraus ergebenden Machtstrukturen geprägt.

Verantwortlich dafür ist vor allem das sogenannte *Mining* (zu Deutsch: schürfen), mit dem Nutzer Bitcoins selbst generieren können. Dafür müssen sie dem Netzwerk einen Teil der Rechenleistung ihrer Computer zur Verfügung stellen. Diese führen dann komplexe Berechnungen durch, mittels derer Transaktionen für gültig erklärt werden. Zur Belohnung für diese für das Netzwerk unentbehrliche Kontrollfunktion erhalten die Anwender neue Bitcoins, die ebenfalls der Blockchain hinzugefügt werden.

In den Anfängen von Bitcoin genügte noch ein einfacher Heim-Computer, um die Berechnungen durchzuführen. Da diese jedoch mit jeder weiteren Transaktion immer komplexer werden, sind dazu heute nur noch industrielle Hochleistungsrechner in der Lage. Neue Bitcoins werden daher inzwischen fast ausschließlich in riesigen, kommerziellen Rechenzentren generiert – den sogenannten *Mining Pools*.

Weil deren Energiehunger gewaltig ist, findet sich die Mehrzahl von ihnen in China, wo Strom vergleichsweise günstig ist. Eine der weltweit größten Anlagen steht in Ordos in der Inneren Mongolei – einst eine florierende Stadt nahe eines riesigen Kohleabbaugebiets. Heute gleicht Ordos einer Geisterstadt. Weil Energie dort aber nach wie vor überaus günstig ist, generieren in den weiten Hallen des Unternehmens Bitmain mehr als 21 000 Rechner Bitcoins; mit 4000 Rechnern wird zudem nach Litecoins, einer anderen Kryptowährung, geschürft. Rund 50 Angestellte sorgen dafür, dass die Computer rund um die Uhr an 365 Tagen im Jahr laufen.⁸ Die gesamte Anlage verbraucht pro Stunde so viel Strom wie 12 000 durchschnittliche deutsche Haushalte im gleichen Zeitraum; pro Tag belaufen sich die Energiekosten auf rund 40 000 US-Dollar. Dennoch lohnt sich das Geschäft: Weltweit werden täglich Bitcoins im Wert von insgesamt mehr als 12 Mio. Dollar generiert.

Schon jetzt kontrollieren vier der größten Mining-Organisationen rund 70 Prozent des Schürfgeschäfts.⁹ Und die Konzentration unter den Minern wird zwangsläufig weiter zunehmen. Denn am Ende verbleiben nur jene von ihnen im Geschäft, die über mehr Rechenkraft und günstigere Energie verfügen als die Konkurrenz. Viel entscheidender aber ist, dass die vier Miner bereits mehr als 50 Prozent der Bitcoin-Transaktionen verarbeiten. Sprächen sie sich ab, könnten sie – so sehen es die Regeln vor – beispielsweise Bitcoins in die eigenen Taschen umleiten. Außerdem können sie mit ihrem Veto jede Änderung an der Bitcoin-Software verhindern.

Die vermeintliche „Befreiungstechnologie“¹⁰ Bitcoin hat aber nicht nur zu einem Oligopol der „Wertschaffenden“ geführt, sondern auch eine globale Besitzelite geschaffen: Gerade einmal 4 Prozent der Nutzerinnen und Nutzer besitzen 96 Prozent des Bitcoin-Vermögens.¹¹ Fernab jeder demokra-

8 Vgl. Zheping Huang und Joon Ian Wong, The lives of bitcoin miners digging for digital gold in Inner Mongolia, www.qz.com, 17.8.2017.

9 Vgl. Nathaniel Popper, How China Took Center Stage in Bitcoin's Civil War, www.nytimes.com, 29.6.2016.

10 Vgl. Larry Diamond, Liberation Technology, in: „Journal of Democracy“, 3/2010, S. 69-83.

11 Vgl. www.howmuch.net/articles/bitcoin-wealth-distribution.

tisch autorisierten Kontrolle haben sie gigantische Reichtümer angehäuft – zumeist ohne dafür auch nur einen Cent an Steuern zu entrichten.¹²

Antidemokratischer Solutionism

Das Bitcoin-Netzwerk ist somit alles andere als sicher und demokratisch. Dass die Macher der Kryptowährung derart kläglich an ihren eigenen utopischen Ansprüchen scheitern, hat sowohl technische als auch politische Gründe.

Zum einen dominieren das Projekt – obwohl es sich als transparent definiert – einige wenige hochspezialisierte Programmierer sowie eine Handvoll überaus mächtiger Miner. Zum anderen bestimmen technische Protokolle und Marktgesetze das Geschehen in der Bitcoin-Welt. Die herrschende Ungleichheit innerhalb des Netzwerks nimmt daher weiter zu, weil das starre, ideologisch unterfütterte Regelwerk derartigen Entwicklungen nicht entgegenwirken kann – und dies auch nicht will. Mit anderen Worten: Es fehlt ein demokratisch reguliertes Korrektiv, das die Übermacht einiger weniger Akteure beschneidet. Bleibt eine solche Regulierung aus, wird die Spekulationsblase unweigerlich weiter anwachsen, die Vermögensungleichheit weiter zunehmen und werden die Miner noch mächtiger werden.¹³

Die Regierungen gehen somit einer Ideologie auf den Leim, die nicht nur ihre staatliche Souveränität im Kern angreift, sondern die obendrein behauptet, komplexe gesellschaftliche Probleme mit Hilfe smarter technologischer Produkte lösen zu können. Das Weltbild des *Solutionism* prägt nicht nur zahlreiche Entwicklungen des Silicon Valleys – für jedes gesellschaftliche Problem eine App –, sondern ähnelt auch dem Konzept des *Social Engineerings*, das bereits in den 1970er Jahren populär war. Schon damals glaubte man, die Gesellschaft nicht mit politischem Handeln, sondern vor allem mittels technokratischer Lösungen optimieren zu können.¹⁴ Die Bitcoin-Währung führt indes allzu deutlich vor Augen, dass dies nicht nur ein gefährlicher, sondern auch ein zutiefst demokratiefeindlicher Irrweg ist.

12 Vgl. Thomas Klemm, Panama für alle, www.faz.net, 18.4.2016.

13 Vgl. Primavera De Filippi und Benjamin Loveluck, The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure, in: "Internet Policy Review", 4/2016.

14 Vgl. Evgeny Morozov, To Save Everything Click Here. Technology, Solutionism, and the Urge to Fix Problems that Don't Exist, London 2014.