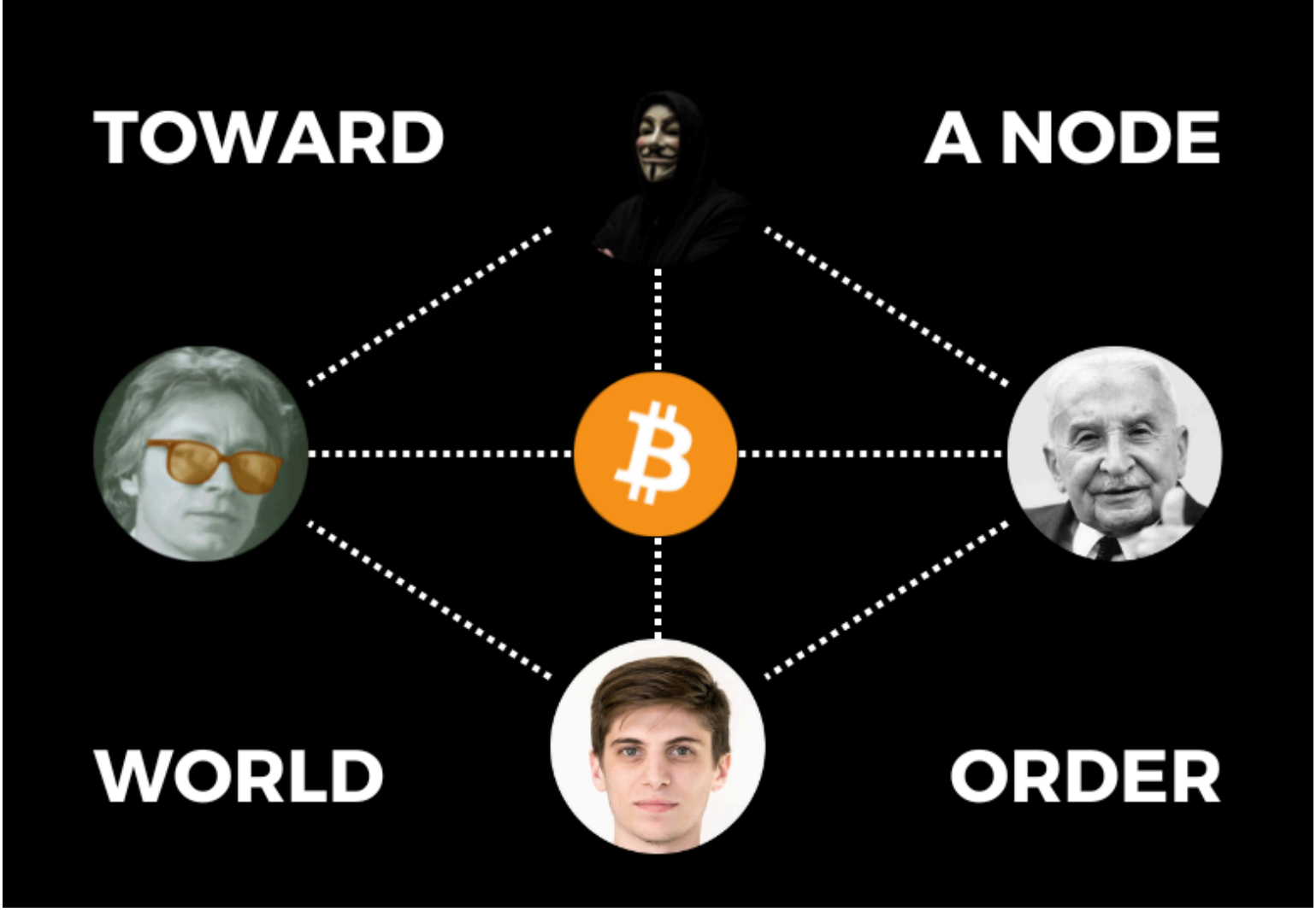
VON MICHAEL GOLDSTEIN

23/02/2023 | Allgemein, Bitcoin, Wirtschaft | 36 min.

Auf dem Weg zu einer Node-Weltordnung

Wie Bitcoin die Inflation überflüssig macht und das menschliche Wohlergehen fördert

Aus dem Original „Toward a Node World Order“ von Michael Goldstein, erschienen am 11. November 2022 auf bitcointimes.com. Übersetzt von DerGeier, Lektorat durch stfano.



„Die ständige Wachsamkeit der Bürger kann das erreichen, was tausend Gesetze und Dutzende von alphabetisch geordneten Ämtern mit Heerscharen von Angestellten nie erreicht haben und nie erreichen werden: die Erhaltung einer gesunden Währung.“

- Ludwig von Mises, The Theory of Money and Credit[1]

Einführung

Der ursprüngliche Zustand des Menschen ist Armut. Die N
unerbittlich in ihrer Knappheit der verfügbaren Mittel. Auf einer be-

stimmten Fläche und mit einer bestimmten Technologie gibt es eine physische Grenze für den Arbeitsertrag. Wie Hans-Hermann Hoppe feststellt:

Für eine solche stationäre Gesellschaft gibt es nur eine Möglichkeit, das reale Pro-Kopf-Einkommen weiter zu erhöhen oder zu wachsen, ohne dass das Pro-Kopf-Einkommen sinkt: durch technologische Innovation, d. h. durch den Einsatz besserer, effizienterer Werkzeuge, die durch Einsparungen ermöglicht werden, die durch den Verzicht auf Freizeit oder anderen unmittelbaren Konsum entstehen.

Er kommt zu dem Schluss, dass es nur durch den Prozess der Senkung der Zeitpräferenz möglich war, aus der Malthusianischen Falle auszubrechen, die durch die Begrenzung der unmittelbar verfügbaren Ressourcen durch den Beginn der industriellen Revolution ausgelöst wurde, um so eine zunehmende Menge an Kapitalgütern und Technologie anzuhäufen.[2]

Ohne ein gewisses Maß an Kapital und Produktion ist der Lebensstandard, den wir für selbstverständlich halten, physisch nicht möglich. Während der industriellen Revolution mussten viele Kinder in gefährlichen Fabriken arbeiten, um das Einkommen der Familie zu sichern. Der Ausweg war das, was George Reisman als „Produktivitätstheorie der Löhne“ bezeichnete. Eine Produktivitätsst[illegible] durch Kapitalakkumulation bedeutet, dass mit jeder verdi[illegible] Geldeinheit mehr Konsumgüter auf dem Markt erworben werden

können. Durch diesen Prozess konnten Familien mit weniger Lohnempfängern genügend Ressourcen erwirtschaften. Die Kinder konnten die Fabriken verlassen und allgemein konnte man sich mehr Freizeit leisten.[3]

Jedoch sind Werkzeuge nur Werkzeuge, und eine staatliche Ideologie kann ihren produktivsten Einsatz verhindern. Mark Thornton weist darauf hin, dass der verabscheuungswürdige Einsatz von Sklavenarbeit, der durch den industriellen Fortschritt in dem oben beschriebenen Prozess zunehmend unrentabel wurde, bis zu seiner gewaltsamen und blutigen Abschaffung aufgrund aggressiver staatlicher Eingriffe in Form von angeordneten Sklavenpatrouillen und dem Verbot der privaten Freilassung von Sklaven in der Praxis erhalten blieb.[4]

Fortschritt scheint also drei Dinge zu erfordern: Kapitalakkumulation, technologischen Fortschritt und eine öffentliche Ideologie, die ihn unterstützt. Es müssen mehr Werkzeuge produziert werden, es müssen bessere Werkzeuge erfunden werden, und die Menschen müssen wissen, wie sie ihre Werkzeuge benutzen können und wollen.

Die Malthusianische Falle ist durchbrochen worden, aber es ist unklar, ob die Menschheit das Potenzial für eine noch weitreichendere Zusammenarbeit hat oder nicht. In Anbetracht der Allgegenwart des Geldes in einer Volkswirtschaft, das als großer Erleichterer [illegible] beitsteilung jede wirtschaftliche Entwicklung ermöglicht, [illegible]ne Technologie, die reif für Innovationen ist.

Der Ursprung des Geldes

In einer Welt der vollkommenen Gewissheit gibt es keinen Bedarf an Geld. Ludwig von Mises beschreibt in *Human Action* den hypothetischen Zustand einer „gleichmäßig ablaufenden Wirtschaft“, in der es keine Veränderungen und somit keine Unsicherheit gibt. In diesem Gleichgewicht gibt es kein Handeln, weil alles Wissen darüber, wann und wie Ressourcen zuzuweisen und auszutauschen sind, bereits bekannt ist.

Doch in der realen Welt kennen wir die Zukunft nicht. Wir sind mit Ungewissheit konfrontiert und haben kaum Mittel, um mit ihr umzugehen. Die Umstände und Präferenzen können sich jederzeit ändern, sowohl bei uns als auch bei anderen. Aus diesem Grund müssen wir uns vorbereiten.[5] Wir können uns nicht auf den direkten Austausch verlassen, um die gewünschten Ressourcen zu erhalten, da das Problem der doppelten Übereinstimmung der Bedürfnisse besteht. Es kann sein, dass andere nicht das haben, was wir wollen, oder dass sie nicht das wollen, was wir haben, und umgekehrt. Um mit dieser Ungewissheit umzugehen, beginnen wir, Güter zu erwerben, nicht um ihrer selbst willen, sondern weil wir glauben, dass sie von denjenigen, mit denen wir tauschen wollen, eher gewünscht werden. Diese Güter können als „Tauschmittel“ klassifiziert werden.

Nicht jedes Gut ist dafür geeignet. Wenn das Gut nicht bes[illegible]st, kann der Akteur nicht sicher sein, dass es zu dem Zeitpunkt, an dem

er in der Zukunft handeln möchte, noch verwendbar ist. Wenn es nicht transportabel ist, könnte es an dem Ort, an dem er in Zukunft handeln möchte, nicht verfügbar sein. Wenn es nicht teilbar ist, kann es sein, dass es nicht in der Menge verfügbar ist, mit der er in der Zukunft handeln möchte. Ein Akteur würde ein Gut wählen wollen, das mit diesen Unsicherheiten am besten zurechtkommt und über die meisten möglichen Zeiträume, Entfernungen und Größenordnungen hinweg verkaufbar bleibt. Wie Mises in *Die Theorie des Geldes und der Umlaufsmittel darlegt, „besteht die unvermeidliche Tendenz, dass aus einer Reihe von Gütern, die als Tauschmittel verwendet werden, die weniger marktgängigen nach und nach verworfen werden, bis schließlich nur noch ein einziges Gut übrig bleibt, das allgemein als Tauschmittel verwendet wird, mit einem Wort: Geld.“*[6]

In der Vergangenheit konzentrierte sich der Wettbewerb um das am besten verkäufliche Gut auf Gold, da es über wünschenswerte physikalische Eigenschaften verfügt: eine geringe Wachstumsrate des Angebots, Langlebigkeit, Formbarkeit usw. Diese Eigenschaften waren damals zwar vorteilhaft, haben aber auf lange Sicht eindeutig nicht ausgereicht.

Der Staat und seine Motivation

Die produktiven Unternehmen sind durch friedliche wirtschaftliche Mittel eingeschränkt, denn sie sind dem Privateigentum v tet, den Launen der Verbrauchernachfrage ausgeliefert und ha e

andere Möglichkeit, als sich durch Senkung der Produktionskosten und Steigerung der Qualität im Wettbewerb zu verbessern. Der Staat hingegen unterliegt solchen Zwängen nicht. Als territoriales Monopol für die endgültige Entscheidungsfindung arbeitet er mit Zwangsmitteln. Einzelpersonen und Unternehmen sind gezwungen, für seine Existenz durch Besteuerung und andere Formen der Enteignung zu zahlen, was *a priori* beweist, dass der Staat keine Leistungen erbringt, die durch friedliche Marktvorgänge tatsächlich nachgefragt werden. Regulatorische und steuerliche Enteignung verschafft dem Staat nicht nur ein Einkommen, sondern auch einen Mechanismus zur Einschränkung des Wettbewerbs.

Wie Hans-Hermann Hoppe jedoch erklärt, kann Gewalt allein nicht den anhaltenden Erfolg eines Staates begründen, und der Staat ist mit einer anderen Art von Zwang konfrontiert, nämlich dem der öffentlichen Meinung.[7] Damit ein Staat so arbeiten kann, wie er es tut,

---

> *„...muss ein Unternehmen neben der Zwangsgewalt auch die Unterstützung der Öffentlichkeit haben. Eine Mehrheit der Bevölkerung muss seine Operationen als legitim anerkennen. Diese Akzeptanz kann von aktiver Begeisterung bis zu passiver Resignation reichen. Aber die Akzeptanz muss in dem Sinne sein, dass eine Mehrheit den Gedan[illegible] aufgegeben hat, sich aktiv oder passiv gegen jeden Ver[illegible] zu wehren, unproduktiven und außervertraglichen Eig[illegible] tumserwerb durchzusetzen. Anstatt sich über solche Aktio-*

nen zu empören, jeden zu verachten, der sie durchführt, und nichts zu tun, um ihnen zum Erfolg zu verhelfen (ganz zu schweigen davon, sie aktiv zu behindern), muss eine Mehrheit sie aktiv oder passiv unterstützen. Die staatstragende öffentliche Meinung muss ein Gegengewicht zum Widerstand der geschädigten Eigentümer bilden, so dass aktiver Widerstand aussichtslos erscheint. Und das Ziel des Staates und jedes Staatsangestellten, der zur Sicherung und Verbesserung der eigenen Position im Staat beitragen will, ist und muss die Maximierung des ausbeuterisch erworbenen Reichtums und Einkommens sein, indem er eine günstige öffentliche Meinung erzeugt und Legitimität schafft.“

Aus diesem Grund hat der Staat ein natürliches Interesse daran, den Wettbewerb einzuschränken, der die Legitimität des Staates bedrohen könnte, sowie „einen Teil des zwangsweise angeeigneten Reichtums an Personen außerhalb des Staatsapparats umzuverteilen und sie dadurch zu korrumpieren [versuchen], damit sie staatsunterstützende Aufgaben übernehmen“. Der Staat zielt zunächst auf die Monopolisierung von Recht und Sicherheit ab, als Mittel zur Durchführung und Durchsetzung der Enteignung, trotz seiner Aggression gegen die natürlichen Eigentumsrechte. Ein weiteres wichtiges Ziel ist die Bildung, um den Bürgern eine ideologische Unterstütz[illegible]len Staat und seine Handlungen einzuprägen.

Die Macht des modernen Staats beruht auf der Monopolisierung eines bestimmten Wirtschaftszweigs: Geld und Banken.

> *„Die Monopolisierung des Geldes und des Bankwesens ist die wichtigste Säule, auf der sich der moderne Staat stützt. In der Tat ist sie wahrscheinlich das am meisten geschätzte Instrument zur Steigerung der Staatseinnahmen geworden. Denn nirgendwo sonst kann der Staat die Verbindung zwischen Umverteilung und Ausgaben sowie Ausbeutung und Rendite direkter, schneller und sicherer herstellen als durch die Monopolisierung von Geld und Bankwesen.“*

Wenn ein Staat eine vollständig monopolisierte Fiat-Währung einführen kann, kann er sie nach Belieben fälschen. Durch Geldinflation in Form von Fälschungen (Produktion von mehr Währungseinheiten ohne zusätzliches Angebot der zugrundeliegenden Ware) kann er indirekt zu geringen Kosten und ohne Angst vor dem Bankrott Reichtum von der Wirtschaft auf sich selbst umverteilen.

Hoppe weist jedoch darauf hin, dass es Hindernisse für den Prozess der Monopolisierung des Geldes gibt. Erstens wird Warengeld durch den Markt erzeugt und nicht durch staatliche Verfügungen. Zweitens ist die Inflation zwar nicht so auffällig wie die Besteuerung, sie wird dennoch wahrgenommen, insbesondere von den Banken. Daher

ist der Staat durch die Herkunft des Warengeldes und die öffentliche Ideologie eingeschränkt, „und daher ist es für den Staat auch unmöglich, mit einer institutionalisierten Geldfälschung durchzukommen, es sei denn, sie kann mit Umverteilungsmaßnahmen kombiniert werden, die in der Lage sind, eine weitere positive Veränderung der öffentlichen Meinung herbeizuführen."

Da Gold historisch gesehen das Geld des freien Marktes war, versuchte der Staat, seine Schwächen auszunutzen, insbesondere seine mangelnde Verkäuflichkeit aufgrund seiner physischen Eigenschaften, die nicht dazu geeignet waren, die wirtschaftliche Unsicherheit zu lindern.

Gold war nicht die Lösung

Hoppe beginnt, den Prozess der Monopolisierung nachzuzeichnen:

> *„In einem ersten Schritt muss die Münzprägung von Gold durch den Staat monopolisiert werden. Dies dient dem Zweck, Gold psychologisch zu verstaatlichen, indem der Schwerpunkt von Gold als universellem Gewichtswert zu Gold als Fiat-Etikett verlagert wird. Und es beseitigt ein erstes wichtiges Hindernis für Fälschungen, weil es dem Staat die institutionellen Mittel an die Hand gibt, sich durch einen systematischen Prozess der Währungsentwertung zu bereichern."*

Gold hat zwar viele attraktive Eigenschaften für Geld, aber die Überprüfung des im Handel erhaltenen Goldes ist sehr kostspielig. Wenn man bedenkt, wie wertvoll eine Sache notwendigerweise sein muss, wenn sie ein allgemein akzeptiertes Tauschmittel ist, ist es nicht nur der Staat, der Geld fälschen möchte. Alle erhaltenen Zahlungen sollten verdächtig sein. Zwar können einige grundlegende Tests von einer normalen Person durchgeführt werden, aber keiner davon ist automatisch. Im schlimmsten Fall, und insbesondere bei großen Zahlungen, muss eine sehr kostspielige chemische Analyse durchgeführt werden, um sicher zu sein, dass man wirklich das Gold hat, von dem man glaubt, es erhalten zu haben, was qualifizierte Fachleute und teure Geräte erfordert. Die hochwertigste Methode ist die Feuerprobe oder Kupellation, bei der das Gold eingeschmolzen, gewogen und neu gegossen werden muss.[8] Dies bedeutet, dass sowohl der Käufer als auch der Verkäufer nicht sicher sein können, dass ein Tausch auch Bestand hat. Der Verkäufer einer Ware kann nicht sicher sein, dass er die volle (oder eine beliebige) Summe an Gold als Bezahlung erhält, und der Käufer kann nicht sicher sein, dass er kein Falschgeld verwendet, nachdem er bei einer früheren Transaktion betrogen wurde.

In der Vergangenheit wurde diese Ungewissheit durch eine Münzprägeanstalt minimiert, die standardisierte Goldmünzen von einer bestimmten Qualität und mit einem erkennbaren und vert[illegible]e-sign herstellen konnte, an dem man sogar erkennen konn[illegible]e Münze manipuliert worden war, z. B. durch Rillen auf der Außenseite,

die verschwinden, wenn jemand versuchte, etwas von der Münze abzuschleifen. Diese Münzstätten verdienten eine Seigniorage, indem sie den Preis der Münzen höher ansetzten als die tatsächliche Metallzusammensetzung. Gleichzeitig konnte dieses Vertrauen in die Münzprägung auch missbraucht werden. Die Münzprägeanstalten konnten Münzen aus dem Verkehr ziehen, die tatsächliche Gold- und Silberzusammensetzung herabsetzen und die Münzen dann mit demselben Preis wieder in Umlauf bringen, wodurch sie durch die Entwertung derselben Münzen mehr Seigniorage einnahmen. Sie könnten dann auch mehr Münzen ausgeben, als es die tatsächliche Metallmenge erlauben würde. Zentralisierte Münzprägeanstalten verringern die Ungewissheit über die Qualität der Ware, aber nur durch die Einführung eines hochgradig vertrauensbasierten zentralisierten Systems, das zu Ungewissheit über die tatsächliche Menge des Metalls in den gehaltenen und in Umlauf befindlichen Münzen und damit über die tatsächliche Geldmenge der gesamten Wirtschaft führt. Da Gold als Ware dezentralisiert ist, gibt es keine Möglichkeit, die Wirtschaft als Ganzes zu überprüfen.

„Zweitens muss die Verwendung von Geldsubstituten anstelle von echtem Gold systematisch gefördert und eine solche Tendenz durch den Erlass von Gesetzen über g setzliche Zahlungsmittel unterstützt werden. Der Fä schungsprozess wird dadurch viel weniger kostspielig. A

statt Gold zu prägen, müssen nur noch Papierscheine gedruckt werden.“

Die teure Lagerung und der teure Transport einer Ware verringern ihre Verkäuflichkeit, da es ungewiss ist, ob die Ware sicher ist, bis sie gebraucht wird, und ob sie zum Zeitpunkt des Umtauschs lieferbar ist. Aufgrund des Gewichts von Gold steigen sowohl die Lagerungs- als auch die Transportkosten im Verhältnis zum Wert des Goldes an. Die langfristige Lagerung erfolgt am besten durch Dritte, die sich die beste Tresortechnologie leisten können, um Diebstahl zu verhindern. Der physische Transport erfordert große Fahrzeuge und Arbeitskräfte. Da es während des Transports auch zu Diebstählen kommt, müssen auch Abwehrmaßnahmen gegen Straßenräuber, Piraten und andere Kriminelle berücksichtigt werden. Der Transport braucht außerdem *Zeit*. Schließlich schränkt die physische Beschaffenheit von Gold auch seine Verkäuflichkeit in kleineren Maßstäben ein. Wenn eine auf Gold basierende Wirtschaft zu wohlhabend wird, wäre es schwierig, physische Goldatome zu verkaufen.

Die Banken lösten dieses Problem, indem sie Geldersatzprodukte in Form von Papierzertifikaten ausstellten. Auch hier konnte Gold nur durch vertrauenswürdige Dritte besser verkauft werden. Die Banken konnten das Gold sicher aufbewahren und die Menschen k
Papierscheine unabhängig von ihrem Wert viel schneller, einfacher

und billiger weitergeben. Dennoch bleibt die Ungewissheit über die Gültigkeit der Papierscheine als solche und darüber, ob diese Scheine tatsächlich Gold in einem Tresor repräsentieren. Die Inflation wird viel einfacher und für jeden vermeintlichen Verwalter von Gold zugänglich. Banken können zwar geprüft werden, aber nicht unabhängig, so dass die Kunden immer darauf vertrauen müssen, dass ihr Gold korrekt behandelt wird, wenn sie sich für eine Bank entscheiden (was praktisch notwendig ist, wenn sie ein gewisses Maß an Handel betreiben wollen). Selbst bei einer solventen Bank bleibt der Zugang zu Gold von einer dritten Partei abhängig.

Sobald die Banken Gold durch Geldsubstitute ersetzt haben, können die Staaten damit beginnen, Gesetze über gesetzliche Zahlungsmittel zu erlassen, um ihre Fälschungsmöglichkeiten zu erhöhen. Der nächste Schritt ist den Bankensektor durch die Einrichtung einer Zentralbank zu einem Kartell zusammenzuschließen. Sobald dies geschehen ist,

---

> *„muss der Staat alle Banken verpflichten, ihr Gold bei der Zentralbank zu deponieren und ihre Geschäfte ausschließlich mit Geldsubstituten statt mit Gold abzuwickeln. Auf diese Weise verschwindet Gold als tatsächlich genutztes Tauschmittel vom Markt und stattdessen werden alltä*

che Transaktionen zunehmend durch die Verwendung von Zentralbanknoten geprägt.“

An diesem Punkt hat der Goldstandard bestenfalls noch seinen Namen. Die Menschen haben ein Geld, das in vielen Dimensionen in Raum und Umfang besser handelbar ist. Theoretisch könnten diese Lösungen von privaten Unternehmen durchgeführt werden, die die Rechte ihrer Kunden respektieren. Die Zentralisierungstendenzen erlauben es dem Staat jedoch, dies zu seinem eigenen Vorteil durch Inflation und Fälschung auszunutzen. Die Banken werden durch die staatliche Kontrolle in Versuchung geführt, weil sie selbst von dem Fälschungssystem profitieren. Nun werden sowohl der Staat als auch die Banken zu ersten Empfängern des neu gedruckten Geldes. Dieser als Cantillon-Effekt[9] bekannte Effekt bedeutet, dass diese Erstempfänger das Geld ausgeben können, bevor die Wirtschaft die Preise an die veränderte Geldmenge anpassen kann.

Die öffentliche Ideologie zur Unterstützung dieses Fiat-Währungssystems beruht also auf zwei Blickwinkeln. Erstens die Tatsache, dass die zugrundeliegende Technologie in vielerlei Hinsicht eine Verbesserung bei der Schaffung eines Geldes darstellt, das besser handelbar ist, mal davon abgesehen, dass ihr ansonsten marktwirtschaftliches Potenzial nun vom Staat vereinnahmt und mo[illegible]siert wurde. Zweitens kann der Staat dies als Vorteil nutzen, indem er

sich selbst zur Quelle des wirtschaftlichen Nutzens macht, was wir an seinen Vermögenswerten sehen, während er die Kosten der Fälschung auf die Wirtschaft überträgt. Da die Banken aufgrund ihrer entscheidenden Rolle bei der Koordination der Wirtschaftstätigkeit naturgemäß eine der mächtigsten Institutionen in einer Volkswirtschaft sind, verschaffen sie der Etablierung einer öffentlichen Ideologie, die die ungerechte Rolle des Staates in der Währungsordnung verteidigt, noch mehr Legitimität und Ressourcen, die deren Fortbestand ermöglichen. So ist es nicht verwunderlich, dass nur wenige gebildete Menschen den Namen Ludwig von Mises während ihres Studiums überhaupt gehört haben dürften.

Die Fiat-Weltordnung

Es ist viel darüber geschrieben worden, was im Jahr 1971 und danach geschah. In diesem Jahr wurde das amerikanische Volk und jeder, der weltweit von der Federal Reserve abhängig ist, einem vollständigen geldpolitischen Experiment unterworfen. Dem Leser wird empfohlen, „Banking, Nation States, and International Politics“ von Hans-Hermann Hoppe zu lesen, um eine umfassendere Studie über den Aufbau dieser Fiat-Weltordnung zu erhalten.

Insbesondere die Fiat-Weltordnung ermutigt Staaten, ihre Macht nicht nur durch militärische Eroberungen, sondern auch durch Geldimperialismus auszuweiten:

„Es liegt im natürlichen Interesse eines Staates, sein Territorium militärisch zu erweitern; daher ist eine Tendenz zur relativen Konzentration von Staaten zu erwarten. Es liegt auch im Interesse eines Staates, einen „Währungsimperialismus“ zu betreiben, d. h. seine Fälschungsmacht auf größere Gebiete auszudehnen; daher ist eine Tendenz zu einer einzigen Papierwährung für die gesamte Welt zu erwarten. Beide Interessen und Tendenzen ergänzen sich gegenseitig. Einerseits ist jeder Schritt in Richtung eines internationalen Fälschungskartells zum Scheitern verurteilt, wenn er nicht durch die Errichtung einer militärischen Dominanz und Hierarchie ergänzt wird. Externer und interner wirtschaftlicher Druck würde das Kartell eher zum Platzen bringen. Mit militärischer Überlegenheit wird jedoch ein Inflationskartell möglich. Andererseits kann der dominante Staat, wenn die militärische Dominanz ein solches Kartell erst einmal ermöglicht hat, seine Ausbeutungsmacht tatsächlich ohne weitere Kriege und Eroberungen auf andere Gebiete ausdehnen. Die internationale Kartellierung der Geldfälschung ermöglicht es dem dominanten Staat, mit raffinierteren (d. h. weniger sichtbaren) Mitteln das zu erreichen, was mit Krieg und Eroberung allein nicht möglich wäre.“

Auf individuellerer Ebene werden Fiat-Bankkonten routin[illegible]aus reiner politischer Laune heraus geschlossen und eingefro[illegible]- lungen an einige Händler und einige Länder sind manchmal nicht er-

laubt, selbst wenn die Transaktion selbst legal ist. Der Zugang zu eigenem Geld ist einfach nicht gegeben.

Trotz alledem entschied sich der Markt in Anbetracht der in der Wirtschaft vorhandenen technischen Möglichkeiten für Gold. Aber genau diese Wahl machte die Wirtschaft anfällig für Fälschungen. Die gleichen Dritten, die notwendig waren, um Gold als Geld zu etablieren, haben auch die Fiat-Weltordnung ermöglicht. Ohne bedeutende technologische Fortschritte konnte kein vernünftiger Ersatz möglich sein, geschweige denn die Unterstützung der Öffentlichkeit gewinnen.

Bitcoin ist die Lösung

„Nur wenn du deine Daten selbst überprüfst und indizierst, kannst du sicher sein, dass deine Indexdaten sicher sind.“

- Satoshi Nakamoto[10]

Im Jahr 2009 befand sich die Wirtschaft bereits mitten in der digitalen Revolution. Eine Reihe von Schlüsseltechnologien waren eingeführt und weit verbreitet worden, darunter Hash-Bäume, Public-Key-Kryptografie, P2P-Netzwerke und SHA-256.[11] Ein bri
pseudonymer Programmierer namens Satoshi Nakamoto
diese Technologien zusammen, um Bitcoin zu schaffen.

Bitcoin löst das so genannte Problem der doppelten Ausgaben ohne eine zentrale Behörde. Jedes andere bestehende digitale Bargeldsystem, einschließlich der heutigen Fiat-Währungen und der darauf basierenden Zahlungsinfrastruktur sowie anderer digitaler Währungen, erfordert eine zentrale Autorität, die die wahre Geschichte eines monetären Kassenbuchs (Ledger) führt und vorgibt, um sicherzustellen, dass dieselben Geldeinheiten nicht zweimal ausgegeben werden. Bitcoin dezentralisiert stattdessen die Buchführung und verwendet ein Proof-of-Work-System, um den Konsens zwischen unabhängigen Buchhaltern über die wahre Geschichte des Kassenbuchs aufrechtzuerhalten.

Ein Bitcoin Full Node ist ein unabhängiger Buchhalter. Er verbindet sich mit dem Bitcoin-Netzwerk, lädt die gesamte Ledger-Historie herunter und validiert jeden Block und jede Transaktion, die er erhält, anhand der von ihm angenommenen Bitcoin-Regeln.[12]

Jeder Full Node arbeitet unabhängig nach seiner eigenen Instanziierung der Software und den darin enthaltenen Regeln. Die Transaktionsinputs müssen kryptografisch mit dem oder den richtigen privaten Schlüssel bzw. Schlüsseln signiert sein. Diese Eingaben müssen auf gültige Transaktionsausgaben zurückgeführt werden können. Der Summenwert der Eingaben muss größer oder gleich dem Wert der Ausgaben sein.

Außerdem müssen die Blöcke gültige Transaktionen beinhalten, deren Inputs noch nicht ausgegeben wurden. Sie müssen einen Verweis auf einen vorherigen gültigen Block enthalten. Sie müssen eine zugehörige Proof-of-Work-Nonce haben, die eine partielle Hash-Kollision mit einem bestimmten Rechenaufwand ermöglicht. Sie dürfen nur eine einzige Coinbase-Transaktion enthalten, die keinen Input hat, aber einen Output, der nicht größer ist als die aktuelle Blocksubvention plus Transaktionsgebühren.

Es gibt noch viele weitere Regeln, die jedes Mal automatisch überprüft werden, wenn eine Transaktion oder ein Block einen Bitcoin-Node erreicht.[13] Zusammengenommen instanziiert der gesamte Node einen automatisierten Buchhalter, der den Willen des Benutzers vertritt, unabhängig von allen anderen im Universum, basierend auf einer bestimmten Konfiguration von Netzwerkparametern seiner Wahl.

Das Bitcoin-Netzwerk wurde so konzipiert, dass ein Full Node in einem Bunker arbeiten kann, abgeschnitten vom Rest der Welt, mit Ausnahme einer einzigen Internetverbindung.[14] Ein Full Node kann alle Daten, die er erhält und die behaupten, ein gültiger Block oder eine Transaktion zu sein, selbst beurteilen. Der Proof-of-Work ermöglicht es dem Full Node, die Daten richtig einzuordnen. Es braucht nur einen einzigen Block mit einem schwierigeren Proof-[illegible], damit der Full Node genau weiß, wie er seine Kopie der Blo[illegible] reorganisieren muss, um wieder in den Konsens zu gelangen. Ein

Eclipse-Angriff, bei dem ein Full Node nur mit gegnerischen Nodes verbunden ist, kann nur so lange aufrechterhalten werden, bis es diesem Node gelingt, einen einzigen 80-Byte-Block-Header zu empfangen, der eine andere Geschichte erzählt. Sobald der Full Node einen Block und Transaktionen empfängt und die Daten validiert, kennt er den Zustand des Bitcoin-Netzwerks, und zwar mit absoluter *Gewissheit*.

Ein Bitcoin Full Node ist eine Maschine der Gewissheit. Wenn ein Benutzer einen Full Node betreibt, erhält er ein Maß an Gewissheit über ein monetäres Netzwerk, das vor der Existenz von Bitcoin kein Mensch hatte. **Jede andere monetäre Technologie ist mit Ungewissheiten behaftet.** Bitcoin löst dieses Problem.

Der Hauptzweck von Bitcoin besteht darin, zwei Probleme zu lösen: doppelte Ausgaben und die Emission. Ersteres wird durch Proof-of-Work-Zeitstempel gelöst. Das zweite Problem wird durch die Schwierigkeitsanpassung und die Coinbase-Transaktionsanforderungen gelöst. Wie wir sehen werden, wurden durch die Lösung dieser beiden Probleme, und zwar auf die Art und Weise, wie Bitcoin sie gelöst hat, die Sicherheitslücken gestopft, die bei früheren Geldtechnologien zu Unsicherheiten führten, die für monopolistische politische Zwecke ausgenutzt wurden.

Der erste Schritt zur staatlichen Kontrolle des Geldes besta[illegible]n, die Münzprägung zu monopolisieren, um ein vertrauenswürdiges

Modell zur Überprüfung der Münzen einzuführen. Bitcoin hat dies durch die Einführung eines kryptographisch sicheren Ledgers gelöst, in dem die Gültigkeit einer Einheit automatisch und sofort überprüft wird. Durch das Betreiben eines Nodes kann ein Nutzer sicherstellen, dass das Angebot und die Qualität aller Einheiten mathematisch einwandfrei sind. Das Angebot wird durch strenge Subventionsregeln für die Coinbase-Transaktion und die Proof-of-Work-Schwierigkeitsanforderungen gesteuert, der zeitliche Ablauf durch die Schwierigkeitsanpassung. Die Empfänger neu ausgegebener Bitcoin-Einheiten können nur dann einen Gewinn erzielen, wenn sie weiterhin kosteneffiziente Energiequellen und Hardware finden können, die starken Wettbewerbskräften ausgesetzt sind, und nicht einfach dadurch, dass ihnen ein gesetzliches Monopol zur Herstellung von Münzen zu einem höheren Preis als ihrem Schmelzwert gewährt wurde. Bitcoin regelt die Seigniorage.

Der zweite Schritt bestand darin, die Verwendung von Geldsubstituten anstelle der Warenwährung selbst zu fördern. Dies ist nicht per se böswillig, denn Geldsubstitute ermöglichen Transaktionen, die aufgrund von Lager- und Transportkosten und mangelnder Teilbarkeit unerschwinglich wären. Es führt jedoch ein notwendiges Gegenparteirisiko für die Bank ein, die die Währung hält, da die Nutzer darauf vertrauen müssen, dass sie die Ware zur Einlösung bereith

Bitcoin hingegen hat Lagerungs- und Transportkosten, di ö-ßenordnungen günstiger sind als Gold. Die Lagerung von Bitcoin er-

fordert im Grunde nur die Fähigkeit, einen 256-Bit-Schlüssel zu speichern. Die Kosten für die Speicherung von Bitcoin-Schlüsseln sind unabhängig vom Wert der Bitcoin, d. h. es spielt keine Rolle, ob die Schlüssel ein paar Satoshis oder ein paar Tausend Bitcoin enthalten. Da es sich um reine Software und Informationen handelt, können innovative Speichermethoden angewandt werden. Während bei allen anderen etablierten Währungen die Einheiten in einem zentralen Tresor oder Hauptbuch gespeichert werden müssen, erkennen die Bitcoin Full Nodes die Verwendung von Transaktionen mit mehreren Signaturen (MultiSig) an und ermöglichen so eine dezentrale Speicherung, die sogar über mehrere Länder hinweg erfolgen kann. Die Schlüssel können auch im Gedächtnis des Nutzers abgespeichert werden, so dass für die Speicherung kein physischer Ort erforderlich ist, was als Absicherung gegen politische Unsicherheiten nützlich sein kann. Bitcoin erfordert auch nicht, dass ein Banktresor geöffnet wird, um mehr Geld einzuzahlen.

Der Transport und die Abrechnung sind viel billiger als bei jedem anderen monetären Netzwerk, einschließlich digitalem Fiat, da sie zwischen zwei beliebigen Schlüsseln überall auf der Welt zu jeder Zeit gegen eine relativ geringe Gebühr erfolgen können. Die Abrechnung kann innerhalb einer Stunde oder sofort über das Lightning-Netzwerk erfolgen. Während bei Gold die Teilbarkeit begrenzt i[illegible]ss es schwierig ist, mit kleinen Goldbeträgen ohne Geldersat[illegible]n-deln, können Bitcoin problemlos in kleinen Beträgen gehandelt wer-

den, insbesondere über das Lightning-Netzwerk, das Beträge unter einem Satoshi ermöglicht. Darüber hinaus basieren die Kosten für den Handel mit der Basiswährung Bitcoin ausschließlich auf dem Datenverbrauch, so dass der Wert von Bitcoin unendlich skaliert werden kann, ohne dass dadurch enorm höhere Kosten entstehen.

Der Betrieb eines Full Nodes ermöglicht es dem Nutzer, seine eigene Bank zu sein, so dass keine Bank als dritte Partei erforderlich ist, die Geldscheine ausgibt, wodurch Fälschungen oder doppelten Ausgaben verhindert werden, es sei denn, eine Person entscheidet sich willentlich, das Gegenparteirisiko einzugehen. Die Einführung eines Geldersatzes, z. B. an einer Börse, kann sich nicht auf das Geld auf systemischer Ebene auswirken, sondern ist nur auf die Nutzer dieses Ersatzes beschränkt. Wenn man eine zweite Ebene wie Lightning als Geldsubstitut betrachtet, kann ein Nutzer seinen eigenen Full Node unterhalten, und jede Einheit ist kryptografisch mit echtem Basisgeld verknüpft, wodurch weiter sichergestellt wird, dass jede Transaktion gemäß der Buchführung des Bitcoin Full Nodes gültig ist. Mit den höheren Erwartungen an eine unabhängig überprüfbare Abrechnung des Basisgelds und bestimmter Geldsubstitute können die Nutzer viel höhere Erwartungen und strengere Anforderungen an Drittanbieterdienste stellen und besitzen mehr Instrumente zur Identifizierung von Fehlverhalten, das im Marktprozess schnell k[illegible] werden kann.

Dies ermöglicht auch eine zensurresistente Integration des Basisgeldes. In einem reinen Fiat-Bankensystem sind alle Zahlungen auf Geldsubstitute angewiesen und erfordern den Einsatz von Gegenparteien, die Transaktionen blockieren und Konten schließen können. Indem man seine eigene Bank ist, können Bitcoin-Nutzer Transaktionen nach Belieben übertragen, und wenn eine ausreichend hohe Gebühr gezahlt wird, kann ein Miner die Transaktion in einen Block mit ausreichendem Proof-of-Work aufnehmen, der wiederum die Blockchain auf allen Nodes aktualisiert, die denselben Regelsatz haben. Wenn man einen Node betreibt, kann man mit der gleichen Gewissheit wie bei jeder anderen Transaktion überprüfen, ob die Zahlung erfolgreich war.

Da von einem Bitcoin Full Node erwartet wird, dass er in einem Bunker arbeiten kann, tendiert die Marktfähigkeit von Bitcoin zur Herstellung von Software, die rückwärtskompatibel ist. Würden sich die Regeln in einer nicht abwärtskompatiblen Weise ändern, müsste ein Nutzer jedes Mal, wenn er sich mit dem Netzwerk synchronisieren möchte, eine vertrauenswürdige Softwarequelle konsultieren, um die richtige Software und die richtigen Regeln zu erhalten. Diese verstärkte Tendenz zur Rückwärtskompatibilität schafft für die Betreiber von Nodes die Gewissheit, dass ihr Verständnis des Netzwerks und insbesondere ihr eigenes Guthaben und ihre Fähigkeit [illegible] Münzen auszugeben, intakt bleiben werden. Dies gilt nicht [illegible] Nutzer von Fiat-Geldsystemen, die aufwachen und feststellen, dass

sie nicht mehr auf ihr Geld zugreifen können, oft ohne Regressmöglichkeit.

Schließlich schafft der Betrieb eines Full Nodes mehr Gewissheit bei der individuellen Kontrolle über die Weitergabe von Identifikationsdaten an Dritte. Das Bitcoin-Netzwerk selbst arbeitet pseudonym, aber im Zusammenhang mit dem Handel können Informationen über den Besitz von Adressen weitergegeben werden, die die Identität, den Kontostand und die Art und Weise, wie Bitcoin gespeichert werden, offenlegen können. Durch die Verwendung eines Full Nodes kann ein Nutzer die Zahl der Informationen, die er für die Verbindung mit dem Netzwerk weitergeben *muss*, reduzieren und so die Ungewissheit verringern, dass bestimmte Informationen veröffentlicht werden, die von böswilligen Nutzern gegen ihn verwendet werden können.

Die neuartige und bahnbrechende Architektur von Bitcoin, die eine unabhängige Eigentümerschaft und Verifizierung ermöglicht, macht die Hauptprobleme, die zur Zentralisierung von Gold geführt haben, vollständig zunichte. Bitcoin hat das Geld repariert, und nun liegt es einfach an den Einzelnen, dies herauszufinden.

Bitcoin Nodes und Methodologischer Individualismus

Die österreichische Schule verwendet den methodologischen Individualismus als eines ihrer Instrumente zur Unterscheidung der Wirtschaftstheorie. Während einige Denkschulen behaupten, dass eine Gruppe einen eigenen Willen haben kann, erkennen die Österreicher an, dass diese Gruppe selbst aus Individuen besteht, deren Handlungen wir analysieren können. Ludwig von Mises schreibt:

> *„Zunächst müssen wir uns bewusstmachen, dass alle Handlungen von Individuen ausgeführt werden. Ein Kollektiv agiert immer durch die Vermittlung eines oder mehrerer Individuen, deren Handlungen auf das Kollektiv als sekundäre Quelle bezogen sind. Es ist der Sinn, den die handelnden Individuen und alle, die von ihrer Handlung berührt werden, einer Handlung zuschreiben, der ihren Charakter bestimmt. Es ist der Sinn, der eine Handlung als die Handlung eines Individuums und eine andere Handlung als die Handlung des Staates oder der Gemeinde kennzeichnet. Der Henker, nicht der Staat, richtet einen Verbrecher hin. Es ist die Bedeutung der Betroffenen, die in der Handlung des Henkers eine Handlung des Staates erkennt. Eine Gruppe von bewaffneten Männern besetzt einen Ort. Es ist der Sinn der Betroffenen, der diese Besetzung nicht den Offizieren und Soldaten vor Ort, sondern ihrer Nation zuschreibt. Wenn wir den Sinn der versch denen Handlungen von Individuen untersuchen, müs wir notwendigerweise alles über die Handlungen von kol-*

lektiven Ganzheiten erfahren. Denn ein soziales Kollektiv hat keine Existenz und keine Realität außerhalb der Handlungen der einzelnen Mitglieder. Das Leben eines Kollektivs wird in den Handlungen der Individuen gelebt, die seinen Körper bilden. Es ist kein soziales Kollektiv denkbar, das nicht in den Handlungen einiger Individuen wirksam ist. Die Realität eines sozialen Ganzen besteht darin, dass es bestimmte Handlungen der Individuen anleitet und auslöst. Der Weg zur Erkenntnis des kollektiven Ganzen führt also über die Analyse der Handlungen der Individuen.“[15]

Und so ist es auch mit Bitcoin. Das Bitcoin-Netzwerk selbst hat keinen eigenen Willen. Es ist eine Ansammlung von Bitcoin-Nutzern, die individuell nach einem gemeinsamen Satz von Netzwerkregeln arbeiten. Jedem Einzelnen steht es frei, sich für die einen oder anderen Regeln zu entscheiden, und das Netzwerk selbst wird durch den Konsens darüber definiert, welche Regeln das sind. Jedes TCP/IP-Netzwerk zwischen zwei oder mehr Computern ist ein Internet, aber nur ein TCP/IP-Netzwerk ist *das* Internet. Gleichermaßen ist jedes Netzwerk von Bitcoin-Nodes *ein* Bitcoin-Netzwerk, aber nur eines ist „*das*“ Bitcoin-Netzwerk.

Wenn eine Person einen Bitcoin Node einschaltet, drückt sie ihren Willen aus, wie die Bitcoin-Regeln aussehen sollen, die mit ihrer Software umgesetzt werden, die keine Ausnahmen zulässt. Die Per-

son muss den Node nur aus reinem Eigeninteresse einschalten. Der Node ist nicht dazu gedacht, die Sicherheit des Netzwerks in einem altruistischen Sinne zu erhöhen, in dem ein zusätzlicher Node zu einer bestimmten Sicherheitsmetrik beiträgt. Stattdessen fügen sie dem Netzwerk einen Ausdruck dessen hinzu, was eine Bitcoin-Einheit definiert, die der Nutzer erhält und ausgibt.

Die Nutzer wählen nicht nur nach den Regeln, die ihnen persönlich wichtig sind. Ein Nutzer würde sich vielleicht wünschen, dass die Netzwerkparameter etwas anders wären, vielleicht mit einer größeren Blockgröße oder einer neuen Transaktionsart. Stattdessen wählen sie die Art und Weise, wie sie ihren Node instanziieren, danach aus, was ihnen am ehesten ermöglicht, den wertvollsten wirtschaftlichen Handel zu betreiben. Eine Funktion, die sie sich wünschen, könnte zwar für sie von Vorteil sein, und auch wenn andere diese Funktion verlangen würden, wenn sie sie richtig verstanden haben, doch falls die Implementierung dieser Funktion einen Konsens mit dem Netzwerk, das ihnen die meisten Möglichkeiten für wertvollen wirtschaftlichen Handel bietet, verhindern würde, könnten sie sich entscheiden, einen solchen Kompromiss zu akzeptieren.

Die Sicherheit des Netzes beruht also nicht auf dem bloßen Betrieb eines Nodes, sondern auf der *Marktfähigkeit*, wie sie von Carl Menger beschrieben wurde. Je mehr Menschen sich dafür entschei des zu betreiben oder sich mit Nodes zu verbinden, die nur ein stimmten Satz von Netzwerkregeln haben, desto mehr Kapazität ge-

winnt das Netzwerk für den wirtschaftlichen Handel. In dem Maße, in dem das Netzwerk mehr Kapazität für den wirtschaftlichen Handel gewinnt, werden sich mehr Menschen dafür entscheiden, Nodes zu betreiben oder sich mit Nodes zu verbinden, die diese Regeln zum Ausdruck bringen. Durch diese Rückkopplungsschleife werden die Regeln, die den Marktbedürfnissen der Menschen am besten entsprechen, weiter gestärkt.

Diese Marktfähigkeit wird in der Wirtschaft über verschiedene Preise signalisiert. Ein Beispiel ist der Preis von Bitcoin-Einheiten. Wenn ein marktfähigeres Netzwerk stärker nachgefragt wird, werden die Einheiten in diesem bestimmten Netzwerk mehr kosten. Empirisch betrachtet können wir beobachten, dass Einheiten aus einem UTXO auf BTC um Größenordnungen mehr verkauft werden als Einheiten aus dem gleichen UTXO auf einem der anderen Forks. Ein weiteres Beispiel ist die Hash-Schwierigkeit. Da Einheiten im Bitcoin-Netzwerk wertvoller sind, sind die Miner bereit, mehr Rechenaufwand zu betreiben, um eine Belohnung zu erhalten. Auch hier zeigt sich empirisch, dass die Schwierigkeit von BTC um Größenordnungen höher ist als die der anderen Forks.

Das Ergebnis ist, wie StopAndDecrypt es nennt, „eine uneinnehmbare Festung der Validierung“. Je mehr wirtschaftliche Aktivitäten durch ein Regelwerk definiert werden, desto weniger Tran[illegible]en und Blöcke, die diesen Regeln widersprechen, können übe[illegible]in das Netzwerk gelangen, da sie von den Nodes zurückgewiesen und

nicht einmal an andere Nodes weitergeleitet werden.[16] Aus den individuellen Entscheidungen von zunächst Tausenden und dann Millionen von Akteuren entsteht ein einziges Bitcoin-Netzwerk, in dem *Buchhaltung mit extremer Befangenheit betrieben* wird und das als allgemein akzeptiertes Zahlungsmittel und -protokoll gilt. *E pluribus unum*.

Bitcoin ist nicht optional

Es gibt kein Bitcoin-Netzwerk außerhalb von Bitcoin Nodes. Diejenigen, die keinen eigenen Full Node betreiben, nutzen den Full Node eines anderen. Wenn eine Person den Full Node einer anderen Person verwendet, vertraut sie den *Behauptungen* dieser Person über den Full Node. Der einzige Weg, um zu wissen, dass man mit Bitcoin so interagiert, wie man denkt, ist, einen Full Node zu betreiben.

Der Besitz von privaten Schlüsseln reicht aus, um jemandem individuelles Eigentum zu ermöglichen, aber nur mit einem Node kann dieser Nutzer die Gewissheit haben, dass die Münzen tatsächlich existieren. Nur über eine Node-Schnittstelle weiß er, dass die mit seinen Schlüsseln verbundenen Adressen UTXOs erhalten haben. Insbesondere weiß er nur über eine Node-Schnittstelle, dass die Adressen UTXOs *in dem Netzwerk erhalten haben, das er meint*. Bei den Schlüsseln kommt es darauf an, dass ein Full Node ihre Beziehung zum Netzwerk kennt.

Keine andere Geldtechnologie bietet solch eine Verkäuflichkeit wie Bitcoin. In einem Fiat-System gibt es weder sinnvolle private Schlüssel noch eine sinnvolle Prüfung des Fiat-Netzwerks. Jeder Akteur, der von den Zusicherungen von Bitcoin profitieren möchte, muss sich am Bitcoin-Netzwerk beteiligen, wenn er sich gegen eine bestimmte Anzahl von Ungewissheiten absichern möchte. Nur wenn man im Besitz von Bitcoin-Schlüsseln ist und einen Bitcoin Full Node betreibt, kann man mit echten Zusicherungen in Bezug auf Eigentum, Knappheit und Zensurresistenz operieren.[17] Das gilt für einen armen Bauern in El Salvador genauso wie für die reichsten Menschen und Institutionen der Welt, einschließlich der Federal Reserve.

Die Errichtung einer Bitcoin-Weltordnung

Auch wenn es widersprüchlich erscheinen mag, dass ein Fiat-basierter Staat ein Interesse an Bitcoin hat, zeigt die Anwendung des methodologischen Individualismus, dass der Staat selbst aus Individuen besteht und nicht aus einem großen Monolithen. Die Individuen, die den Staat bilden, haben immer noch ihre eigenen monetären Bedürfnisse und Interessen. Selbst dort, wo Bitcoin die Macht des Staates einschränken könnte, könnten die Individuen selbst davon profitieren, was es unwahrscheinlicher macht, dass sie an einem Angriff auf Bitcoin interessiert sind.[18] Staaten und Supermächte selbst bleiben in einem anarchischen *Verhältnis zueinander*.[19] Sie müssen m- weise immer noch mit anderen Nationen Handel treiben o- kurrenzfähig bleiben. Kleinere Nationen, die selbst nicht die Macht

haben, Geld zu drucken, könnten auf Bitcoin setzen, um einen langfristigen Vorteil und Unabhängigkeit zu erlangen, wie in El Salvador zu sehen. Überall dort, wo Handel und Ersparnisse mit Ungewissheiten konfrontiert sind, ist ein monetärer Vermögenswert erwünscht, der diese Ungewissheiten ausgleichen kann. Auch wenn Staaten dem Bitcoin ablehnend gegenüberstehen, können wir sehen, dass sie nicht allmächtig sind und sich genauso wie wir mit einer sich verändernden Wirtschaft und technologischen Durchbrüchen auseinandersetzen müssen. Wenn Bitcoin tatsächlich eine globale Reservewährung werden kann, braucht die Federal Reserve ihren Full Node und ihre Coldcard genauso wie irgendein „toxischer Bitcoin-Pleb".

Das soll nicht heißen, dass alle Staaten, von den schwächsten bis zu den dominantesten, sich morgen einfach dem Bitcoin hingeben werden. Es zeigt uns lediglich, dass im monetären Wettbewerb mehr im Spiel ist als nur rohe Gewalt. Bei der Betrachtung des monetären Wettbewerbs wurde an anderer Stelle viel über das wirtschaftliche Potenzial von Bitcoin, eine globale Reservewährung zu werden, geschrieben,[20] aber über das ideologische Wachstumspotenzial von Bitcoin wurde weniger gesagt.

Bitcoin löst in seinem Kern drei Probleme auf dezentrale Weise: Eigentum durch Public-Key-Kryptographie, doppelte Ausgaben durch Proof-of-Work-Zeitstempel und Emission durch Proof-o[illegible]-Schwierigkeitsanpassung. Da das System auf extremem ge[illegible]schen Denken basiert, wird *jeder* erfolgreiche Angriff als fataler Feh-

ler des Bitcoin-Systems angesehen. Diese Probleme sind wiederum nur Teilaspekte von größeren Problemen: staatliche Enteignung und Fälschung. Jedes Mal, wenn Bitcoin seine Verteidigung gegen die unbedeutenden Versionen der Probleme stärkt, hat es auch die Abwehrmechanismen gegen die abscheulichsten Versionen der Probleme aufgebaut.

Jeder Angreifer, ob gegenwärtig oder in Zukunft, ob technisch oder ideologisch, hat es mit einem System zu tun, das bereits seine Verteidigungsmechanismen gegen ihn aufgebaut hat. Jeder erfolgreiche Angriff, der Bitcoin nicht vernichtet, dient nur dazu, dem Rest des Netzwerks beizubringen, wie man sich in Zukunft besser gegen ihn und ähnliche Angriffe schützen kann. Man kann mit keiner Hashleistung erzwingen, dass ein ungültiger Block ins Netzwerk kommt, so dass – als die Befürworter von SegWit2x damit drohten, eine Hard-Fork-Kette zu minen – weitere Bitcoiner lernten, wie wichtig es ist, sich auf ihren eigenen Node anstatt auf den eines anderen zu verlassen.[21] Als Börsen gehackt oder Lending-lattformen liquidiert wurden, lernten weitere Bitcoiner, wie wichtig es ist, ihre eigenen Schlüssel zu besitzen. Dies geschah aus umsichtigen wirtschaftlichen Motiven, um mehr Gewissheit über ihr Geld zu haben, aber es stärkt wiederum auch die Verteidigung gegen größere Akteure, die die gleichen Angriffe in größerem Maßstab durchführen wollen.

Mittlerweile bietet Bitcoin eine einzigartig leistungsfähige r-käufliche Geldtechnologie, um Ungewissheiten zu verringern, die die

Menschheit seit Jahrhunderten verfolgt haben, sowie Möglichkeiten, die ihn für ein zunehmend internetverbundenes Zeitalter noch besser geeignet machen. Da es sich bei Bitcoin um eine reine Software handelt, ist er zudem noch leistungsfähiger geworden und verspricht, dies auch weiterhin zu werden. Jeder Akteur, der funktionierendes Geld benötigt, d. h. jeder Akteur in einer entwickelten Arbeitsteilung, braucht Bitcoin. Je weiter die Akzeptanz voranschreitet, desto mehr Menschen verlassen sich auf das Netzwerk und desto ernster nehmen alle Teilnehmer die Lösungen, die durch die selbstverantwortliche Teilnahme angeboten werden, sowie die Behebung potenzieller Schwachstellen für zukünftige Angriffe.

Letztendlich wird jeder, der gutes Geld braucht, von Bitcoin angezogen, und jeder, der von Bitcoin angezogen wird, ist auch gewillt, Bitcoin zu verteidigen. Das Wirtschaftswachstum und der Wille, Bitcoin zu sichern und zu verteidigen, sind miteinander verwoben. In einem brillanten Aufsatz, „The Will To Be Free: The Role of Ideology in National Defense“,[22] betrachtet Jeffrey Rogers Hummel die Frage, wie eine hypothetische zukünftige staatenlose Gesellschaft die Verteidigung gegen Angriffe von außen sicherstellen würde:

> *„Allein durch den Sturz der einheimischen Regierung [illegible] friedlich oder gewaltsam) haben die ehemaligen Unte[illegible] nen mächtige Instrumente geschaffen, um sich vor fre[illegible] den Regierungen zu schützen. Derselbe soziale Konsens,*

dieselben Institutionen und dieselben ideologischen Imperative, die ihnen die Befreiung von ihrem eigenen Staat ermöglicht haben, wären automatisch vorhanden, um sich gegen andere Staaten zu verteidigen, die versuchen, das Vakuum zu füllen.“

Bei jedem Schritt des Bitcoin-Wachstums muss eine neue Gruppe von Personen die Ungewissheiten, mit denen sie in der Welt zu tun haben, abwägen und überlegen, ob Bitcoin ihre Probleme lösen kann. Selbst wenn sie zunächst nicht zustimmen, muss jeder damit beginnen, jede Änderung des Bitcoin-Status quo der Souveränität, die einen Full Node und die Verwahrung privater Schlüssel erfordert, durch die Linse von „Bitcoin oder Shitcoin?“ zu betrachten. Unter rein wirtschaftlichen Betrachtungen wird bei der Frage, welchen Vermögenswert man für monetäre Zwecke auswählen soll, Bitcoin die folgerichtige Antwort sein. Diejenigen, die sich aus irgendeinem Grund für Bitcoin entscheiden, begeben sich auf einen Weg, der zwangsläufig ihre Entschlossenheit stärkt, Bitcoin genauso zu belassen, wie er ist, was von Natur aus eine implizite oder explizite Haltung gegen jegliche Doppelausgaben und Fälschungen ist.

Diejenigen, die sich für Bitcoin entscheiden, erleben einen dramatischen langfristigen Anstieg der Kaufkraft ihrer Ersparniss höhen die Gewissheit über den Zustand und den Wert ihre s und ihres monetären Netzwerks, den Zugang zu ihren finanziellen

Mitteln und die Fähigkeit zur Liquidation. Jedes Wachstum ist ein Zeichen für einen Erfolg, der dazu dient, die Glaubwürdigkeit für andere zu erhöhen, und jedes enorm riesige Wachstum ist ein Zeichen für die gleiche, wenn nicht noch größere Leistungsfähigkeit. Ausgehend von einem einzigen Nutzer hat dieser Prozess zu einem globalen Netzwerk mit Tausenden von Nodes, Hunderten von Milliarden Dollar an Wert und ganzen Nationalstaaten geführt. Mit der Zeit gibt es nur noch eine Antwort auf die Frage „Bitcoin oder Shitcoin?“

Nachdem der Grundstein gelegt war, um die Probleme des Eigentums, der doppelten Ausgaben und der Emission auf allen Angriffsebenen zu lösen, musste das Bitcoin-Netzwerk wirtschaftlich stark genug werden, um die Menschen zu ermutigen, es als Geld wertzuschätzen. Und die Fähigkeit von Bitcoin, diesen Angriffen standzuhalten und eine globale Reservewährung zu werden, erforderte genügend Leute, die Schlüssel besitzen und Full Nodes betreiben, um eine solche Ordnung aufrechtzuerhalten.

Eine Bitcoin-Strategie für den Weltfrieden

Nach der Schaffung einer neuen globalen Reservewährung, die auf einer in allen Dimensionen überlegenen Geldtechnologie beruht, wird die Menschheit auf ein grundlegend besseres Wirtschaftssystem umgestellt haben. Die Unzulänglichkeiten des Goldes werden beben sein und die Einfachheit und die Vorteile des Fiat-Geldes werden übernommen werden, ohne dass vertrauenswürdige Dritte erforder-

lich sind. Die Wirtschaft würde dank einer größeren und kooperativeren Arbeitsteilung schneller wachsen, was wiederum zu weiteren Software-Innovationen, die die technologischen Fähigkeiten von Bitcoin stärken, führen könnte.

In einer solchen zukünftigen Welt wird die Abhängigkeit von Bitcoin zwangsläufig zunehmen und die Wirtschaftsakteure in einer Kultur verankern, die alles Notwendige tut, um die Sicherheit von Bitcoin zu gewährleisten.

Da es keine Möglichkeiten mehr für doppelte Ausgaben und Fälschungen gibt, wird das Geldmonopol des Staates wegfallen, da niemand mehr eine Nachfrage nach seinen Dienstleistungen haben wird. Ohne das profitabelste Mittel zur Umverteilung von Reichtum wird dies zu einer höheren Produktivität in der Wirtschaft führen, da weniger Ressourcen von produktiven Unternehmungen abgezogen werden. Dieses Wachstum wird durch die Tatsache verstärkt, dass die gleichen Ressourcen nicht an Menschen und Institutionen umverteilt werden, die diese Ressourcen nutzen, um ideologische Unterstützung für die Umverteilung selbst zu schaffen. Militärische Eroberungen werden weniger, da die Kosten des Krieges direkter bezahlt werden müssen, und der Währungsimperialismus hat keinen Zweck, da kein Volk bereit ist, einen Shitcoin anzunehmen.

Diejenigen, die bisher dazu neigten, ihre Unternehmen durch Fälschungen und Inflation zu finanzieren, haben nun einen alternativen

Mechanismus, der ihr Handeln lenkt. Vor allem weil die Produktionskapazität der Wirtschaft immer schneller zunimmt, bedeutet die steigende Kaufkraft jeder Bitcoin-Einheit, dass jeder Möchtegern-Inflationist nun wählen muss, ob er Bitcoin hodln oder einen Kampf gegen ein Geldsystem aufnehmen will, das unschlagbar ist.

Seit dem Genesis-Block von Bitcoin muss die Menschheit ihr Vertrauen nicht mehr in Dritte setzen, um ein so wichtiges Instrument wie Geld zu verwalten. Die Menschen können nun ihre eigenen Nodes betreiben und ihre eigenen Schlüssel besitzen, um ihr Geld ständig zu überwachen und es nach eigenem Ermessen zu verwenden. Die industrielle Revolution hat die Menschheit aus der Malthusianischen Falle befreit. Bitcoin, der der Fälschung ein für alle Mal ein Ende bereitet hat, befreit uns aus der Fiat-Falle.

Michael Goldstein

@Bitstein

Oktober, 2022

Fußnoten

1. „The Return to Sound Money" aus *The Theory of Money and Credit* von Ludwig von Mises.↩
2. Siehe „From the Malthusian Trap to the Industrial Rev[illegible]An Explanation of Social Evolution" aus *The Great Fiction* v[illegible]s-Hermann Hoppe.↩

3. Siehe *Capitalism* von George Reisman, S. 621. Siehe auch „Prices, Wages, and Labor“ in „*The Church and the Market*” von Thomas E. Woods, Jr., und „How Capitalism Enriched the Working Class” in „*How Capitalism Saved America*” von Thomas J. DiLorenzo.↩
4. „Slavery, Profitability, and the Market Process” von Mark Thornton.↩
5. Mehr über Geld als Absicherung gegen künftige Ungewissheit in „The Yield from Money Held‘ Reconsidered” von Hans-Hermann Hoppe. Mehr darüber, wie sich die Qualität eines Geldes auf seine Kaufkraft auswirkt, siehe „The Quality of Money” von Philipp Bagus.↩
6. Siehe auch „On the Origins of Money” von Carl Menger, und „The Fiat Standard” von Saifedean Ammous.↩
7. „Banking, Nation States, and International Politics: A Sociological Reconstruction of the Present Economic Order” von Hans-Hermann Hoppe. Siehe auch „How is Fiat Money Possible?—or, The Devolution of Money and Credit” von Hoppe und „What Has Government Done to Our Money?” von Murray Rothbard.↩
8. Unter „The gold standard” in *Chemistry World* findet man einen Einblick in die Arbeit, die nötig ist, um herauszufinden, ob Goldbarren wirklich aus Gold bestehen.↩
9. Siehe „How Central Banking Increased Inequality“ von Louis Rouanet.↩
10. „Gepostet auf Bitcointalk” am 25. November 2010.↩
11. Siehe „Bitcoin is Worse is Better“ von Gwern Branwen.↩

12. Ein Pruned-Node kann Daten verwerfen, die bereits verifiziert wurden und für eine weitere Verifizierung nicht mehr benötigt werden, aber Archivierungsnodes behalten ganze Kopien der Blockchain für eine dauerhafte Aufzeichnung.↩
13. Eine detailliertere Aufschlüsselung der Validierung von Transaktionen und Blöcken findet man unter „Protocol Rules" im Bitcoin Wiki.↩
14. Siehe „Proof That Proof-of-Work is the Only Solution to the Byzantine Generals' Problem" von Oleg Andreev. Man beachte, dass zusätzliche Verbindungen zum Bitcoin-Netzwerk von Vorteil *wären*, um bestimmte Arten von Angriffen zu verhindern.↩
15. „The Principle of Methodological Individualism" in *Human Action* von Ludwig von Mises.↩
16. „Bitcoin Miners Beware: Invalid Blocks Need Not Apply" von StopAndDecrypt.↩
17. Siehe diesen Reddit-Beitrag von Pieter Wuille über die Bedeutung des Betriebs und der Verwendung eines eigenen Full Nodes.↩
18. Siehe „Bitcoin's Shroud of Subtlety and Allure" von Daniel Krawisz.↩
19. Siehe „Do We Ever Really Get Out of Anarchy?" von Alfred G. Cuzán.↩
20. Siehe „The SNI Mempool Crash Course in Political Economy" „The Bitcoin Standard" von Saifedean Ammous, und „[illegible]ish Case for Bitcoin" von Vijay Boyapati.↩
21. Siehe „The Blocksize War" von Jonathan Bier.↩

22. Neu veröffentlicht in „The Myth of National Defense: Essays on the Theory and History of Security Production", herausgegeben von Hans-Hermann Hoppe.↩

Dies ist ein Beitrag von Michael Goldstein auf bitcointimes.com. Die geäußerten Meinungen sind ausschließlich seine eigenen und spiegeln nicht notwendigerweise die von Aprycot Media wider.

Vielen Dank fürs Lesen! Aprycot Media kümmert sich darum, guten Bitcoin-Content auf Deutsch verfügbar zu machen. Ob einzelne Artikel, Bücher oder eine ganze Mediensammlung.

Die Inhalte auf der Mediathek werden von unseren Übersetzern und Lektoren, unseren Content Plebs, auf freiwilliger Basis und unentgeltlich erstellt. Wenn du ihnen etwas zurückgeben möchtest, findest du auf https://aprycot.media/content-plebs/ die Möglichkeit, ihnen ein paar Sats zukommen zu lassen. #value4value

Eine noch umfangreichere Übersicht findest du unter: aprycot.media/thek/ oder auch bitcoinquellen.de.

Das Buch Satoshis

€25,68

Enthält 7% MwSt.

zzgl. Versand

Lieferzeit: ca. 2-3 Werktage (DE)

AUSFÜHRUNG WÄHLEN

Coinfinity Bitcoin Blinks

€14,00

Enthält 7% MwSt.

zzgl. Versand

Lieferzeit: ca. 2-3 Werktage (DE)

AUSFÜHRUNG WÄHLEN

Hoodie – Print Books. Not Money.

Die Orange Pille

€16,99 – €24,00

0

€89,00

Enthält 19% MwSt.
zzgl. Versand

Lieferzeit: ca. 2-3 Werktage (DE)

AUSFÜHRUNG WÄHLEN

Enthält 7% MwSt.
zzgl. Versand

Lieferzeit: ca. 2-3 Werktage (DE)

AUSFÜHRUNG WÄHLEN

WEITERE ARTIKEL

Warum Bitcoin die optimale Kreditsicherheit ist

Aus dem Original „Why Bitcoin Is Pristine Collateral“ von Leon Wankum, erschienen am 13. September 2022 auf Bitcoin Magazine.Dieser Artikel erklärt, warum die Eigenschaften von Bit-

“Das Bitcoin-Diplom” gratis bei Aprycot

Das Bitcoin-Diplom ist das Schulbuch, das in El Salvador im Unterricht eingesetzt wird. Heute veröffentlichen wir die dt. Übersetzung.

Kapital im 21. Jahrhundert

Geld ist eine emergente Ordnung, deren Funktionsweise Allen Farrington nachgeht.

0

coin zu seiner unvermeidlichen Verwendung als Sicherheit für die Kreditvergabe führen, hauptsächlich aufgrund seiner Überlegenheit...

ZUM ARTIKEL

ZUM ARTIKEL

ZUM ARTIKEL

DISCOUNTS UND MEHR IM NEWSLETTER

Mail-Adresse

ANMELDEN

Quick Links

Buchhandel

Partner

Content Plebs

Kontakt

Shop

Allgemeine Geschäftsbe[illegible]un-gen

Wider[illegible]rung

Zahlungsweisen

0

Versand & Lieferung

Konto

Gutschein Saldo

Wir sind ein deutscher Verlag, der sich auf Bitcoin-Literatur spezialisiert hat. Hier findest du von Büchern, über Blog-Posts bis hin zu einer umfangreichen Linksammlung alles was du brauchst um Bitcoin besser zu begreifen.

0