

BRETT SCOTT

VISIONEN EINES LEVIATHANS

DIE POLITISCHEN IMPLIKATIONEN DER BITCOIN-TECHNOLOGIE

In Kim Stanley Robinsons epischem Roman «Red Mars» aus dem Jahr 1993 errichtet eine Gruppe von WissenschaftlerInnen auf dem Mars eine Kolonie. Manche von ihnen begreifen die Kolonie als Chance auf ein neues Leben, das nach gänzlich anderen Regeln funktioniert als jenen, die auf der chaotischen Erde herrschen. Doch mit der Zeit übernehmen multinationale Konzerne, die im Mars nur ein weiteres Geschäftsfeld sehen, die Kontrolle, etablieren eine Regierung, und die Hoffnung zerplatzt. Dies ist ganz sicher eine Geschichte, mit der sich viele aus der Bitcoin-Gemeinde identifizieren können. Die Vision, die dahinter steht, scheint heute bedroht zu sein: eine digitale Ökonomie, die auf einer Kryptowährung basiert und die unabhängig von den Entscheidungen aufgeblähter Banken und aggressiver Regierungen agieren kann. Hier soll es darum gehen, was den Kern der Bitcoin-Innovation ausmacht – und um die Frage, ob sie das Empowerment-Versprechen hält, das seine BefürworterInnen ihr zuschreiben.

Für viele Außenstehende sind Bitcoins eine kuriose Modeerscheinung, ein Fehlzünder, der bald der Medienlangeweile zum Opfer fallen wird. Doch das ist ein Irrtum. Im Kern der von Bitcoin geleisteten Innovation steckt weit mehr als nur eine neue Währung. Deshalb wird sie auch nicht einfach wieder verschwinden. Mit Bitcoin ist nicht nur ein Zahlungsmittel entstanden, sondern eine Methode zur Erstellung eines dezentralen, von den NutzerInnen selbst gesicherten, mit Datum und Uhrzeit versehenen Registers. Oder noch einfacher gesagt: Bitcoin ist eine Methode zur Vermeidung zentralisierter Speicherstellen. Solche Stellen sind in der Gesellschaft omnipräsent, von den Banken, die elektronische Transaktionen zwischen mir und meinem Vermieter aufzeichnen, über das Patentamt, dessen MitarbeiterInnen das Datum einer Erfindung registrieren, bis hin zu den Parlamentsakten, die die Verabschiedung neuer Gesetze dokumentieren. Am Sichtbarsten wird diese technische Innovation jedoch im Bereich der Währung.

Banken verwalten Informationen. Die Zeiten, in denen UnternehmerInnen einen Haufen Gold zur sicheren Aufbewahrung in den Tresorraum ihrer Bank brachten, sind lange vorbei. Wenn Sie heute «350 Euro auf der Bank» haben, bedeutet das einfach, dass diese Zahl in der Datenbank des Rechenzentrums Ihrer Bank gespeichert und Ihrer Kontonummer zugeordnet ist. Bei einer elektronischen Überweisung schicken Sie Ihrer Bank im Prinzip nur eine Nachricht. Sie identifizieren sich über Ihre PIN oder Kartenummer und bitten darum, den Eintrag in der Datenbank um den genannten Betrag zu ändern und die Bank des Empfängerkontos über die «Zahlung» zu informieren, damit diese den Betrag dem Empfängerkonto gutschreibt. Als Gruppe betrachtet, besitzen kommerziel-

le Banken somit ein Monopol zur Speicherung von Transaktionsdaten. Auf diese Weise können sie nachvollziehen, «wie viel Geld wir haben». Ein von derartigen Banken losgelöstes und gleichzeitig sicheres elektronisches Währungssystem müsste daher Antworten auf drei miteinander zusammenhängende Fragen geben. Erstens: Wie lassen sich die von den Banken kontrollierten privaten Datenbanken ersetzen? Zweitens müsste geklärt werden, wie sich Informationen in diesen Datenbanken «manipulieren» lassen (wie sich also «Geld bewegen» lässt). Und drittens müsste die Frage beantwortet werden, wie man die Menschen davon überzeugt, dass die umherbewegten Einheiten auch tatsächlich etwas wert sind.

Bitcoin löst das erste Problem durch eine öffentliche Datenbank, ein Buchungssystem: die «Blockkette». Die am Bitcoin-System Beteiligten können Informationen in diesem Buchungssystem speichern. Aber sobald eine Information gespeichert ist, kann sie nicht mehr bearbeitet werden.¹ Ein verteiltes Kollektiv von Kontoristen «verleiht» im Prinzip seine Rechenkraft und hält das Buchungssystem kollektiv aufrecht, indem es die eingehenden Daten zu abgeschlossenen Transaktionsketten «verwebt». Diese KontoristInnen werden *Miners* (dt. SchürferInnen) genannt. Zweitens verfügt Bitcoin über einen Prozess zur Identifikation von NutzerInnen, damit diese bei den KontoristInnen Transaktionen in Auftrag geben und ins Buchungssystem eintragen lassen können. Hier kommt die Verschlüsselung der Daten ins Spiel: Meinen öffentlichen Bitcoin-Schlüssel (in etwa vergleichbar mit einer Kontonummer) kontrolliere ich über meinen privaten Schlüssel (im Prinzip wie meine Konto-PIN). Im Zusammenspiel dieser beiden Elemente eröffnet sich anonymen Individuen die Möglichkeit zur anonymen Aufzeichnung von Transaktionen

untereinander in einer Datenbank, die von einem dezentralen Netzwerk betrieben und gesichert wird. Das dritte Element, also Menschen davon zu überzeugen, dass die gehaltenen Einheiten tatsächlich etwas wert sind, ist eine etwas subtilere Frage, mit der ich mich an dieser Stelle nicht weiter beschäftigen werde.

Dieser Ansatz hat unmittelbare politische Implikationen. Im Bitcoin-System wird die Gruppe mächtiger zentralisierter InformationsvermittlerInnen (das über die Zentralbank miteinander verbundene und von den Regierungen gestützte Monopol der Banken) durch ein diffuseres Netzwerk ersetzt, bei dem auf den ersten Blick niemand die direkte Kontrolle hat. Von einer solchen Idee fühlen sich all jene angezogen, die die Macht der Banken durch eine größere Vielfalt im monetären System begrenzen möchten. Leute mit links-anarchistischen Einstellungen, die im Staat und im Bankensektor die VertreterInnen derselben elitären Interessen sehen, mögen in einem solchen System das Potenzial zu einer direkten und kollektiven demokratischen Kontrolle von Geld erkennen. Wirklich angesprochen hat die Idee allerdings vor allem liberale Konservative, die in Bitcoins eine warenartige Währung sehen, die frei ist von den Übeln der Einmischung durch Zentralbanken und Regulierung.²

Die politischen EntscheidungsträgerInnen und das ökonomische Establishment lassen bisher drei Reaktionen erkennen: Zunächst sind da Bedenken, dass Bitcoins zur Geldwäsche und für kriminelle Aktivitäten genutzt werden könnten. Zweitens bestehen Sorgen um den Verbraucherschutz. Schließlich ist da noch die Frage der Steuern. Allerdings bereitet die engstirnige Sichtweise der Aufsichtsbehörden, die sich ausschließlich auf die potenziell negativen Auswirkungen von Bitcoin konzentrieren, aber zugleich für die Schwächen des derzeitigen Währungssystems blind bleiben, den Boden für die politische Auseinandersetzung um das Zahlungssystem. Bitcoin-BefürworterInnen, die die von ihnen geschaffene Nische leidenschaftlich verteidigen, werden auch wegen dieser Ignoranz empfänglich für Verschwörungstheorien, nach denen angeschlagene Banken bei Regierungen eifrig für ein Verbot von Bitcoin werben und paranoide PolitikerInnen in Panik um die Integrität der nationalen Währung geraten.

Fernab des Medienhypes um diese Bitcoin-Dramen formiert sich jedoch eine wesentlich tiefer greifende Bewe-

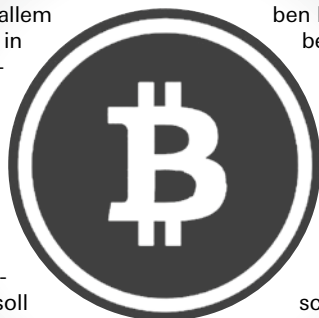
gung. Diese betrachtet dezentralisierte Blockketten nicht nur als Möglichkeit, Geschäftsbanken zu entmachten, sondern als potenziellen Weg, auch andere Formen der zentralisierten Verwaltung von Informationen obsolet zu machen. Ein Beispiel aus dem Urheberrecht: Urheberrechtsinstitutionen speichern derzeit Ansprüche auf die Urheberschaft an einem bestimmten Werk zu einem bestimmten Datum und fügen dem Werk einen entsprechenden offiziellen Stempel an. Diese zentralisierte «Zeitstempelung» wird «Notarisierung» genannt. Eine nichtmonitäre Anwendung einer Blockkette, die auf den gleichen Prinzipien wie Bitcoin basiert, könnte daher sein, die privat kontrollierten Bücher von NotarInnen durch eine öffentliche Notarisierung zu ersetzen, mit der Personen ihre Ansprüche dokumentieren können.³

Und wie steht es mit DNS-Einträgen (Domain Name System) zur Registrierung von Internetadressen? Tippt man eine URL wie www.seite-xy.de ein, steuert der Browser zunächst eine private Datenbank (ein DNS-Register) an, in der die URLs IP-Adressen (den Adressen bestimmter Geräte bzw. Empfänger) zugeordnet sind, an die man dann weitergeleitet wird. Man könnte aber genauso gut ein dezentrales Register von Domain-Namen-BesitzerInnen über eine Blockkette organisieren.⁴ Theoretisch ließe sich auf diese Weise der Besitz von Aktien, Land, eigentlich jeder Besitz als solcher aufzeichnen.⁵

Bei der Frage, wer die größten VerwalterInnen von Informationen sind, sehen wir den Wald oft vor lauter Bäumen nicht. Zum Beispiel Facebook: Ist das nicht einfach ein Unternehmen, dem man Informationen schickt, die dann in Facebooks Datenbanken gespeichert und anschließend Ihnen und Ihren FreundInnen angezeigt werden? Man loggt sich mit einem Passwort ein (wodurch man sich identifiziert) und ändert die Datenbank sodann durch das Senden weiterer Informationen (etwa: «Ich möchte dieses Foto wieder löschen»). Gleiches gilt für Twitter, Dropbox und unzählige weitere webbasierte Dienste. Anders als das ursprüngliche Internet, das vor allem der Übertragung statischer Inhalte diente, erleben wir heute Seiten wie Facebook als interaktive Spielwiesen, auf denen wir auf weit entfernten Computern installierte Programme nutzen. Bei dieser Art von Interaktivität vertrauen wir Unternehmen wie Facebook riesige Mengen an Informationen über uns an. Auf der Grundlage dieser Informationen können uns Firmen gezielt Dinge verkaufen – das ist das Geschäftsmodell, mit dem Plattformen wie Facebook ihre Profite ma-

BITCOIN ist ein seit dem Jahr 2009 verfügbares, weltweites Zahlungssystem. Die einzelne Geldeinheit in diesem Zahlungssystem heißt ebenfalls Bitcoin. Der gängigste Weg, Bitcoins zu erwerben, ist es, sie auf Bitcoin-Marktplätzen im Internet zu kaufen. Bisher wird mit Bitcoin vor allem im Internet bezahlt, vereinzelt gibt es aber auch in der Gastronomie oder im Einzelhandel die Möglichkeit, Rechnungen mit Bitcoin zu begleichen. Der Kurs dieser «Währung» unterliegt starken Schwankungen.

Das Besondere an dem Zahlungssystem ist, dass es auf einer dezentralen Datenbank, der sogenannten Blockkette (engl. *block chain*), basiert. Sie wird gemeinsam von den NutzerInnen verwaltet, in ihr werden alle Transaktionen verzeichnet. Diese dezentrale Datenbank soll eine Einflussnahme von staatlicher Seite oder eine Regulierung durch Banken unmöglich machen. Ohne eine zentrale Autorität soll so ein weltweiter Zahlungsverkehr ohne zeitliche Verzögerung und mit nur sehr geringen Gebühren ermöglicht werden, der auch ohne eine vor Ort vorhandene



Bankeninfrastruktur funktioniert. Hierbei kommen kryptografische Techniken (technische Verfahren zur Verschlüsselung von Informationen) zum Einsatz, weshalb Bitcoin auch als «Kryptogeld» oder «Kryptowährung» bezeichnet wird. Neben Bitcoin gibt es noch eine Reihe weiterer, wenig bekannter Kryptowährungen.

Die Gesamtgeldmenge im System ist auf 21 Millionen Bitcoin begrenzt. Derzeit sind etwa 13,8 Millionen Bitcoin im Umlauf. Durch das sogenannte *Mining* (dt. Schürfen) werden – mittels des dezentralen Einsatzes von Rechenleistung – neue Blöcke der Blockkette erzeugt. Dadurch werden auf der einen Seite getätigte Transaktionen bestätigt und im System verzeichnet und gleichzeitig neue Bitcoins geschöpft. Das *Mining* ist sehr rechenintensiv, da sich der notwendige Einsatz an Rechenleistung dynamisch an die Gesamtrechenleistung des Systems anpasst, sodass nur etwa alle zehn Minuten ein neuer Block erstellt wird. Für jeden neu erstellten Block werden 25 neue Bitcoins geschöpft, bis zur Maximalsumme von 21 Millionen Bitcoins. Patrick Stary

chen. Darüber hinaus können Behörden wie die NSA den so entstandenen Informationsspeicher durchforsten. Was aber wäre, wenn sich interaktive Web-Dienste entwickeln ließen, die nicht auf einem zentralen Informationsvermittler wie Facebook aufbauen? Genau hieran arbeiten Gruppen wie Ethereum.⁶ Stellt Bitcoin eine Form der dezentralen Aufzeichnung von einfachen Transaktionsinformationen dar, zielt Ethereum auf die Schaffung einer «dezentralen Rechenmaschine». Auf einem solchen System ließen sich Programme oder Verträge über eine Blockkette ausführen, die von einem verteilten Netzwerk von Computern anstatt von Mark Zuckerbergs Rechenzentren zusammengehalten würde.

Allmählich hört sich das alles nach Science Fiction an, aber Organisationen wie Ethereum arbeiten tatsächlich an vorderster Front am Aufbau «dezentralisierter autonomer Organisationen», programmierter Objekte also, mit denen Menschen interagieren können, die aber von niemand Bestimmtem kontrolliert werden. Einem solchen Gebilde kann ich Informationen schicken, wodurch die programmierten Funktionen aktiviert und weitere Aktionen in Gang gesetzt werden. Wie Bitshares es beschreibt, verfügen solche Organisationen über «einen in Open-Source-Software kodierten Business-Plan, der völlig automatisch und in transparenter und vertrauenswürdiger Weise ausgeführt wird».⁷

Mark Zuckerberg von Facebook oder Jamie Dimon von JP Morgan sind die menschlichen Gesichter hinter den digitalen Schnittstellen ihrer Dienste. Sie können Daten offen manipulieren oder sich dem Druck der Zensur beugen. Allem Anschein nach wäre eine dezentralisierte Währung oder eine dezentralisierte Version von Twitter solchen Eingriffen gegenüber immun.⁸ Gerade auf diesem Punkt baut das Narrativ des Empowerments auf, und in der Tat bieten diese Überlegungen auf den ersten Blick eine aufregende Vision autonomer Außenposten der Freiheit in einer ansonsten von großen und korrupten Institutionen dominierten Welt. Die Blockkette kann Verträge zwischen freien Individuen aufzeichnen. Sollten sich Mechanismen zur Durchsetzung dieser Verträge schaffen lassen, hätten wir ein System zum Aufbau von Gesetzen, das keinen Staat braucht. Wenn es nach den VordenkerInnen der Blockketten-Technologien ginge, würden sie das heutige System ersetzen, da diese Technologien in jeder Hinsicht den bestehenden Institutionen gegenüber überlegen sind. Nehmen wir die Idee allerdings etwas genauer unter die Lupe, wird aus dem scheinbar utopischen Projekt schnell eine Anti-Utopie mit konservativem Einschlag.

Fragt man die BefürworterInnen von Bitcoins, warum ihre Währung anderen überlegen ist, hört man häufig, dass Bitcoins «vom Problem des Vertrauens befreit»⁹ seien: Es bedürfe keines Vertrauens in fehlbare «Regierungen und Konzerne». An die Stelle des Vertrauens trete ein von Individuen geschaffenes, selbsterhaltendes System, das einem festgelegten, von menschlichen Schwächen oder menschlicher Einmischung unabhängigen Satz von Regeln folge. Ein solches System sei fairer, weil es Menschen in die Lage versetze, sich gegen jene durchzusetzen, die die Macht haben, Regeln zu missbrauchen.

Auffällig an dieser «Vision» ist ihre Skepsis gegenüber allen menschlichen Eigenschaften. Während sich anarchistisch inspirierte PhilosophInnen alternative Formen gesellschaftlicher Organisation zumeist auf der Grundlage von Basisgemeinschaften vorstellen, die gemeinschaftliche Beziehungen aufbauen, geht es der Bitcoin-Gemeinde um autonom agierende Individuen, die mit anderen autonomen

AkteurInnen auf der Grundlage fest codierter Regeln zusammenarbeiten. Diese Regeln sind es, die sie vor denjenigen schützen, die ihren Interessen entgegenstehen. In dieser Vorstellung schwingt eine Verachtung menschlicher Unvollkommenheit mit, insbesondere der Unvollkommenheit der Mächtigen, implizit aber auch der von uns allen. Wir müssen vor uns selbst geschützt werden, indem wir Macht an einen automatisch ausgeführten Code delegieren. Die Bitcoin-Gemeinde scheint nicht an die Veränderbarkeit von Institutionen zu glauben, sondern sich vielmehr von einer Art Anti-Politik angezogen zu fühlen, bei der Handlungen auf binär kodierte Alternativen beschränkt sind. Hierin kommt eine konsumorientierte Sicht auf die Welt zum Ausdruck, in der man sich nicht «ausdrückt», indem man debattiert oder verhandelt, sondern indem man ein Produkt einem anderen Produkt vorzieht. Die Vision entpuppt sich als ein befremdliches, spannungsgeladenes Amalgam aus überschwänglicher, risikofreudiger Freiheit einerseits und risikoscheuer, antisozialer Paranoia andererseits.

DER MYTHOS VOM POLITISCHEN AUSSTEIGEN

BefürworterInnen verbinden mit Bitcoin die Möglichkeit, aus dem bestehenden System auszusteigen. Aber wohin eigentlich? Die Vorstellung eines Ausstiegs ins Internet ist bizarr, weil das Internet von massiven Investitionen des Staates und der Konzerne in die physische Infrastruktur abhängig ist, von auf dem Meeresboden verlegten Glasfaserkabeln, der Massenproduktion von Computern durch schlecht bezahlte ArbeiterInnen in Fernost und vom breiten Wohlstand in den Ländern des Westens. Die eine Seite des krypto-anarchistischen Mantras «Schutz der Privatsphäre der Schwachen und Transparenz für das Agieren der Mächtigen» ist an und für sich ein gesunder radikaler Impuls. Konservativ wird es, sobald allein der Schutz der Privatsphäre soziales Empowerment ermöglichen soll. Die Annahme, dass Empowerment vor allem daraus erwächst, in Ruhe den eigenen individuellen Interessen nachgehen zu können, ist im Kern die Ideologie der bereits Mächtigen, nicht die der Schwachen.

Die gleiche Ambivalenz findet sich in der verwandten Cypherpunk-Szene.¹⁰ Häufig wird sie als eine radikale Befreiungsbewegung dargestellt, doch genauer betrachtet, bietet die Welt der Kryptografie-Freaks keineswegs die Möglichkeit, den Dynamiken der Macht zu entkommen. Die Flucht führt nur unter die Herrschaft eines anderen Satzes von Regeln, die zwar nicht von «PolitikerInnen» kontrolliert werden, aber dafür in den Händen von ProgrammiererInnen und den EigentümerInnen von Rechenkapazität liegen. Vor diesem Hintergrund erscheint Bitcoin nicht als ein Reich, das ohne staatliche Regeln auskommt, sondern als eines, das seine eigenen Regeln durchsetzt. Es bietet Schutz, aber garantiert keineswegs Empowerment oder den Ausstieg aus dem Bestehenden.

Technologie erscheint oft als leise und unbewegt, eine Welt der apolitischen Objekte. Wir neigen daher dazu, den Dynamiken der Macht gegenüber blind zu sein, die in ihre Nutzung eingeschrieben sind. Sind beispielsweise E-Mails nicht einfach ein praktisches Werkzeug? Tatsächlich ist es höchst fraglich, ob wir noch die Wahl haben, E-Mail zu nutzen oder nicht. Klar, ich kann mich zwischen Gmail und Hotmail entscheiden, aber die breite Verwendung von E-Mails schafft Netzwerkeffekte, sodass langfristig der Verzicht auf die Nutzung von E-Mails immer weniger eine Option ist. Diejenigen, die nicht mitmachen, werden marginalisiert –

schon dieser Umstand macht aus der Technologie eine politische Frage. Dieser Punkt ist wichtig. Während einzelne Blockketten-Technologien ganz offensichtlich nützlich sein könnten, bergen sie als Technologien, die auf die Unterstützung menschlicher Interaktionen ausgelegt sind, die latente Gefahr einer technokratischen Entwicklung. Losgelöst von den ProgrammiererInnen, die sie entwickelt haben, können Blockketten, wenn sie erst einmal Einzug in die Abläufe der zwischenmenschlichen Beziehungen gehalten haben, schnell zur Schreckensvision einer Unterwerfung des Menschen unter Algorithmen werden. Dies fing Joseph Lubin vom Ethereum-Projekt (vermutlich unabsichtlich) ein, als er sagte: «Es wird möglich sein, Leute zu manipulieren, damit sie schlechte Entscheidungen treffen, aber es wird nicht möglich sein, das System an sich zu manipulieren.»¹¹

Interessanterweise weist diese Abstraktion Parallelen zu Thomas Hobbes auf. In seiner Schrift «Leviathan» versteht er den egozentrischen Menschen, dass es in seinem besten Interesse ist, einen Teil seiner Freiheit gegen die Sicherheit von Leib und Besitz einzutauschen. Hierzu schließt er einen Vertrag mit einem gottgleichen Souverän, der die gesellschaftlichen Spielregeln festlegt. Mit der Zeit wurde die Definition dieses Souveräns aufgeweicht, wie auch die Fiktion, dass Menschen tatsächlich einen Vertrag mit ihm eingehen. Dennoch bildet diese Vorstellung das Fundament der modernen Erwartung, dass die Regierung Eigentumsrechte zu sichern habe. Libertäre Konservative halten an dem Glauben fest, dass die Aufstellung klarer Eigentumsrechte und klarer Vertragsregeln die Garantie für die Entstehung optimaler Systeme sei. In diesem Sinne unterscheiden sie sich nicht groß von Hobbes. Allerdings stört sie an Hobbes, dass seine Vision Vertrauen in PolitikerInnen setzt, die als Menschen nicht wie ein unabhängiger Vertragssouverän agieren, sondern dazu neigen, an den Regeln herumzupfuschen, Dinge zu verbessern oder «zu klauen». Bieten dezentrale Blockketten da nicht endlich die Aussicht auf geschützte Eigentumsrechte mit klaren Regeln und ohne politische Einmischung? Im Kern ist dies die Vision eines technologischen, internetbasierten Leviathans, eines auf den Rang eines Gottes gehobenen Krypto-Souveräns, an dessen Regeln wir uns vertraglich binden können. Die Regeln sind eine Reihe von Algorithmen, schrittweise Kalkulationen, die sich nur sehr schwer ändern lassen. Zu Beginn repräsentieren sie vielleicht, im Rousseau'schen Sinn, den Gemeinwillen aller am Vertragsnetz Beteiligten. Der springende Punkt ist aber, dass ein Ausbrechen aus einem einmal in diesem System geschlossenen Vertrag kaum möglich ist.

Natürlich spricht eine solche Vision vor allem diejenigen an, die glauben, dass mächtige Institutionen in erster Linie dadurch funktionieren, dass sie Eigentumsrechte, Verträge und Regeln missachten. Doch während eines Großteils der jüngeren Geschichte war das zentrale Problem mit mächtigen Institutionen nicht ihre Bereitschaft, Verträge zu verletzen, sondern vielmehr, sie als unveränderbar darzustellen. Verträge sind im Wesentlichen nichts anders als Algorithmen, codierter Ausdruck der je nach Umständen erwünschten Resultate. Für gewöhnlich werden sie von TechnokratInnen geschrieben, und für gewöhnlich spiegeln sie die Interessen der gesellschaftlichen Elite wider. Gerade deshalb sind Befreiungsbewegungen immer darum bemüht, die Verträge vorangegangener Regime zu brechen, seien es Bauernbewegungen, die sich weigern, die Schuldverträge mit LandbesitzerInnen einzuhalten, sei es die Demokratische Republik Kongo, die alte, von multinationalen Konzernen gehaltenen Bergbaukonzessionen infrage stellt.

Beim politischen Befreiungskampf geht es sowohl um das Anfechten als auch um das Durchsetzen von Verträgen.

EINE TECHNOLOGISCH-POLITISCHE VISION

Man entflieht der Welt der großen Konzerne und Regierungen nicht mit dem Wunsch nach einer Welt, in der Technologien herrschen, die in ihrer Gesamtheit einen technokratischen Krypto-Souverän ergeben. Stattdessen müssen wir Technologien im kontinuierlichen politischen Kampf nutzen und gleichzeitig nie aufhören, diese kritisch zu hinterfragen. Das Konzept dezentraler Blockketten ist ein mächtiges Konzept. Die kalte, argwöhnische Seite von Cypherpunk leistet aber nur dann einen Beitrag zu Empowerment und Befreiung, wenn sie im Dienst kreativer, warmblütiger, fest in der schmutzigen physischen Welt verankerter menschlicher Gemeinschaften steht. Statt auf die Speicherung digitaler Güter oder digitalen Eigentums in Form von Blockketten sollten wir uns auf den Einsatz von Blockketten in güterlosen Systemen konzentrieren. Ein Beispiel ist das Potenzial von Blockketten für Systeme zur Stimmabgabe,¹² denn zentrale Behörden zur Stimmauszählung sind ein bekanntes Sorgenkind in politisch instabilen Ländern. Wie wäre es, die ausgezählten Stimmen in einem von BürgerInnen betriebenen dezentralen Netzwerk zu speichern und WählerInnen die Möglichkeit zu geben, ihre Stimmen anonym an eine öffentliche Datenbank zu übermitteln? Das Ziel kann weder eine Gesellschaft sein, die frei von Menschen ist, denen wir vertrauen müssen, noch eine, in der sich unsere politischen Hoffnungen im Schutz der Privatsphäre erschöpfen. Stattdessen sollten wir auf eine Welt hinarbeiten, in der wir Technologie nutzen, um die Macht von Systemen zu untergraben, die uns an der Möglichkeit vertrauensvoller Beziehungen zweifeln lassen.

Brett Scott ist Journalist und Autor des Buchs «The Heretic's Guide to Global Finance. Hacking the Future of Money» (London 2013). Er bloggt unter www.suitpossum.blogspot.com und twittert als @suitpossum.

¹ Diesen Punkt kann man gar nicht genug betonen, denn er bedeutet, dass Informationen in Blockketten weder nachträglich zensiert, also gelöscht, noch manipuliert, also verändert werden können. ² In konservativ-libertären Kreisen dominieren häufig die Vorstellungen österreichischer Ökonominnen von «sicherem Geld». Gold, Silber und andere nur beschränkt verfügbare Güter werden als «echtes» Geld angesehen – im Gegensatz zum «betrügerischen» Fiatgeld der Regierungen und zum Geld der Geschäftsbanken unter dem Mindestreserve-System. Solche Kreise betrachten Bitcoin als digitale Form des Goldes. ³ Genau hieran arbeiten die Projekte Proof of Existence (www.proofofexistence.com) und Originstamp (www.originstamp.org). ⁴ Vgl. etwa Namecoin unter: www.coin-desk.com/what-are-namecoins-and-bit-domains. ⁵ Siehe zum Beispiel das Mastercoin-Projekt unter: www.mastercoin.org. ⁶ Vgl. www.ethereum.org. ⁷ Vgl. <http://bitshares.org>. ⁸ Vgl. z. B. das Projekt Twister unter: <http://twister.net.co>. ⁹ Vgl. <http://www.thebitcoinsociety.org/content/bitcoin-beauty-trustless-transactions>. ¹⁰ Cypherpunk ist eine Anti-Überwachungs-Bewegung, die die Nutzung von Kryptografie zum Schutz vor den Schnüffeleien der Behörden propagiert. ¹¹ Vgl. www.theepochtimes.com/n3/665367-bitcoin-2-0. ¹² Mit solchen Systemen experimentiert z. B. die Gruppe Restart Democracy; vgl. <http://restartdemocracy.org>.

IMPRESSUM

STANDPUNKTE wird herausgegeben von der Rosa-Luxemburg-Stiftung und erscheint unregelmäßig V. i. S. d. P.: Henning Heine
Franz-Mehring-Platz 1 · 10243 Berlin · www.rosalux.de
ISSN 1867-3163 (Print), ISSN 1867-3171 (Internet)
Redaktionsschluss: März 2015
Lektorat: TEXT-ARBEIT, Berlin
Satz/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf Circleoffset Premium White, 100 % Recycling