Rainer Rehak

Die Blockchain: Das Recht der (Rechen-)Stärkeren

Vom Experiment einer Gesellschaft ohne Vertrauen

Es ist eine der Aufgaben der kritischen Informatik, informationstechnische Artefakte bezüglich ihrer gesellschaftlichen und sozialen Implikationen kritisch zu analysieren. Der besondere Beitrag besteht darin, auch technisch detaillierte Problem- und Konfliktfelder aufzuzeigen – etwa indem eingeschriebene Welt- und Wertvorstellungen expliziert werden – und diese dadurch sozialwissenschaftlich untersuchbar und diskutierbar zu machen. Dies soll hier am Beispiel der Blockchain versucht werden. Dieser Artikel erschien auch gekürzt in den WZB-Mitteilungen Nr. 161, September 2018.

Die Blockchain ist in aller Munde und hat das verlockende Versprechen, die Intermediäre gesellschaftlicher Interaktionen überflüssig zu machen. Diesen muss aktuell vertraut werden, was große Abhängigkeiten schafft, wie die Bankenkrise schmerzlich bewies. Etwa Notariate oder Banken würden durch die Blockchain überflüssig. Doch die Macht der Akteure löst sich ob der blockchain-immanenten technischen Dezentralisierung und Unveränderbarkeit nicht auf, sondern verschiebt sich nur hin zu anderen, neuen und vor allem illegitimen und unkontrollierten Machtzentren. So interessant die Blockchain technisch ist, sie ist kein Ersatz für klassische politische Gestaltung und Regulierung von Macht.

Moderne Gesellschaften basieren auf Vertrauen – in andere Menschen, aber auch in Verfahren wie demokratische Wahlen oder in vermittelnde Institutionen wie etwa Banken. Ohne dieses generalisierte Vertrauen könnten komplexe, arbeitsteilige Gesellschaften nicht existieren. Gelegentlich wird dieses Vertrauen jedoch fundamental enttäuscht, und so liegt es nahe, nach neuen Wegen zu suchen, um die Notwendigkeit von Vertrauen im gesellschaftlichen Miteinander zu minimieren. Aktuell werden dafür primär neue Digitaltechnologien wie die sogenannte Blockchain in den Blick genommen, wie sie in Bitcoin oder Ethereum Anwendung findet. Diese soll – richtig angewendet – zentrale Intermediäre, sogenannte vertrauenswürdige Dritte wie Banken oder genereller: Notare, überflüssig machen. Die Blockchain soll demnach das Problem der Abbildung eines gemeinsamen Konsenses neutral technisch-kryptografisch lösen und nicht mehr organisational.

Technisch gesehen ist die Blockchain ein Verfahren, um das in der Informatik *network consensus* genannte Problem zu lösen. Dabei geht es darum, verlässlich und manipulationssicher eine gemeinsame Sicht auf den jeweiligen Gegenstandsbereich herzustellen. Klassische Beispiele für dieses Problem sind die Zeitsynchronisation oder die Zuweisung von Domainnamen zu IP-Adressen. Aber auch die gemeinsamen Protokollierungen von Aktivitäten oder Wert- beziehungsweise Geldtransaktionen, bei denen es zusätzlich eine Geschichte gibt, gehören dazu. Wie kann sich ein Netzwerk von verteilten Systemen darauf einigen, was aktuell „in der Welt der Fall" ist? Die einfachste Lösung für dieses Problem sind zentrale Stellen, die den jeweiligen Zustand im Auftrag der beteiligten Systeme verwalten und so aufwandsarm und skalierbar Kohärenz herstellen können. Letztendlich wird damit jedoch die gesamte Macht über das System an eine oder wenige privilegierte zentrale Stellen delegiert, denen alle Beteiligten vertrauen müssen und die im besten Falle kein Eigeninteresse an einer Manipulation haben. Mit der Blockchain soll die Machtkonzentration und Verwundbarkeit zentraler Ansätze durch technisches Erzwingen von Dezentralisierung, öffentlicher Nachvollziehbarkeit und Verunmöglichung nachträglicher Veränderung verhindert werden. Die Blockchain bietet also die Funktionalität eines Verzeichnisses ohne Intermediäre, weshalb oft auch der Begriff „vertrauenslos" (trustless) fällt.

Wie kam es zu der weltweiten Verbreitung dieser Technologie? Kann sie die hehren Versprechen ihrer Anhängerschaft auch im praktischen Einsatz halten? Das für die Blockchain relevante Vertrauensthema wurde 2008 durch die Bankenkrise und die daraus resultierende weltweite Rezession virulent. Die zentralen Institutionen – in diesem Falle Banken – hatten sich massiv selbst bereichert, relevante Kennzahlen manipuliert und so ein weltweites Finanz- und Vertrauensfiasko produziert, dessen Auswirkungen auch heute noch global zu spüren sind. In der Folge wurde die Bankenregulierung jedoch weder nennenswert verschärft, noch wurde eine Zerschlagung der Großbanken diskutiert. Die Verursacher wurden mit Steuergeldern gerettet und konnten im Wesentlichen weitermachen wie bisher, während weltweit die Wirtschaften ächzten und Millionen Menschen ihr Hab und Gut verloren. Diese (Nicht-)Reaktion staatlicher Stellen auf eines der relevantesten Ereignisse der jüngeren Wirtschaftsgeschichte bescherte einer Strömung innerhalb der Technikgemeinde immensen Aufwind: Die sogenannten *crypto-libertarians* fühlten sich bestätigt, dass jegliche Machtkonzentration mehr schadet als nützt – das Einzige, was zählt, ist das Individuum. Dieses könne und müsse sich mit technischen Werkzeugen, insbesondere kryptografischen, gegen die übergriffigen Institutionen wehren. Auch wenn diese Bewegung schon seit Jahrzehnten existierte, stießen ihre radikal-individualistischen Überzeugungen nun auf immer mehr offene Ohren außerhalb der eigenen Reihen. In diesem Klima veröffentlichte eine Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto ein Konzeptpapier für ein alternatives globales Zahlungsmittel – samt benutzbarer Software inklusive der kryptografischen Mechanismen. Die Kryptowährung *Bitcoin* war geboren, ein öffentliches, verteiltes Überweisungsverzeichnis mit dem Anspruch, keine Intermediäre zu kennen; ein Geldsystem ohne Banken also.

Diese Technologie kann natürlich nicht nur für die Verarbeitung von Finanztransaktionen verwendet werden, sondern für jegliche Transaktionen und durch die Unveränderbarkeit der Historie auch zum verlässlichen Speichern beliebiger Informationen inklusive ausführbarer Programme. Diese Abstraktion und Generalisierung von Bitcoin führte zur Blockchain-Technologie, die nun, ähnlich einem Notariat, zur Verarbeitung beliebiger Transaktionen verwendet werden kann. Um die fast schon magisch anmutende Zuschreibung zu analysieren, dass ein neutral-technisch dokumentierter Konsens hergestellt werden kann, soll

der Mechanismus der Blockchain kurz dargestellt werden. Die Blockchain besteht aus einer chronologisch geordneten Kette von Dateneinheiten, den sogenannten Blöcken, wobei ein Block jeweils eine Anzahl von Transaktionen und einen kryptografisch sicheren Verweis auf den vorherigen Block enthält. Die Block-Kette enthält also die aktuell gültige Geschichte des Netzwerks. Ein Block kann dabei nachträglich nicht geändert werden, weil sonst die nachfolgenden Blöcke ungültig würden.

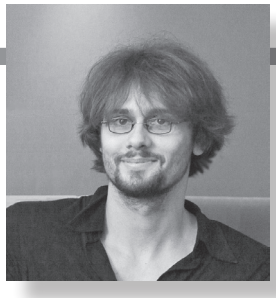
Die Brillanz der Blockchain besteht darin, dass alle Computer des Netzwerks gleichzeitig versuchen, aus den bislang nicht in Blöcken festgehaltenen Transaktionen den neuen Block zu formen, sie lösen also gleichzeitig eine kryptografisch aufwendige Aufgabe. Sobald der erste Computer sie gelöst hat, müssen alle auf Basis dieses nun entstandenen Blocks den nächsten Block erstellen. Bei Bitcoin geschieht dies ungefähr alle zehn Minuten. Die immense Ressourcennutzung im Wettbewerb des parallelen zufälligen Durchprobierens – das sogenannte Mining – soll sicherstellen, dass es immer ein anderer Computer des Netzwerks ist, der den nächsten Block erzeugt. Wenn jemand also bestimmte Blöcke manipulieren will, um eine alternative Geschichte zu schreiben, müsste es dieser Akteur mit dem Rest des Netzwerks aufnehmen können. Dieses Konkurrenzmodell begründet die Verteiltheit des Systems. Da es jedoch eine rechenintensive Aufgabe ist, steigt die Lösungswahrscheinlichkeit mit der Rechenleistung des eingesetzten Computers.

Bei der Betrachtung und Kontextualisierung der technischen Eigenschaften fällt auf, dass die Blockchain zwar technisch dezentral konzipiert ist, dabei aber – wie bei individualistischen Herangehensweisen üblich – von gleich mächtigen Akteuren ausgeht. Da aber die Blockgenerierung etwa bei Bitcoin innerhalb des Netzwerks finanziell honoriert wird, hat schon seit mehreren Jahren eine Professionalisierung der Miner in Form von Zusammenschlüssen und Hardwareaufrüstung stattgefunden. Handelsübliche Laptops treten nun gegen mit Grafikkartenchips hochgerüstete Rechencluster an – und verlieren praktisch immer. Denn allein die Rechenkraft ist für die Verteilung der Blockgenerierung ausschlaggebend; das System hat also keinen internen Mechanismus, die anfängliche Dezentralisierung auch aufrechtzuerhalten. Aktuell befinden sich je nach Schätzung 50 bis 60 Prozent der sogenannten *hash rate*, also der Rechenleistung des gesamten Bitcoin-Netzes, in den Händen der chinesischen Miner-Firma Bitmain. Dieser Grad der Zentralisierung ist vergleichbar oder sogar größer als der im konventionellen Bankensystem. Im größten aktiven Blockchain-Projekt ist Dezentralisierung also eine Illusion. Zwar sind die Manipulationsmöglichkeiten begrenzt (so können etwa Transaktionen nur verzögert oder ganz unterdrückt werden), aber diese Begrenzung ergibt sich eher aus der Öffentlichkeit der Kontoführung und der darunterliegenden asymmetrischen Kryptografie, die auch ohne Blockchain verwendet werden kann; die Begrenzung kommt gerade nicht vom (de-)zentralen Charakter. Und noch ein weiterer Faktor kommt hinzu, wenn Dezentralisierung nur technisch angegangen wird. Stehen in einem Netzwerk 90 Prozent der einzelnen Computer unter Kontrolle einer Person oder Organisation, mag das Netzwerk aus technischer Sicht immer noch verteilt sein, die Machtanalyse ergibt jedoch ein ganz anderes Resultat. Dies relativiert die Erwartungen an jegliche blockchainzentrierte Lösung gewaltig.

Auch die Analyse der Unveränderbarkeitseigenschaft der Blockchain ist in politischer Hinsicht aufschlussreich. Das Konzept einer kryptografisch sicheren Protokollierung ist in Informatikzeiträumen gedacht schon alt. Sie wird mindestens seit den 1980er Jahren praktisch angewendet, etwa in Form sogenannter *hash chains*. Neu ist tatsächlich der verteilte Charakter, doch dieser bringt ganz eigene Nebeneffekte mit sich. So führte 2016 ein Programmierfehler zu zwei parallelen unterschiedlichen Historien der blockchain-basierten Kryptowährung Ethereum, die mühsam wieder zusammengeführt werden mussten. Auch absichtlich werden Blockchain-Historien modifiziert oder besser gesagt gespalten: 2016 wurde eine vollautomatische kommerzielle Organisation namens DAO entwickelt, deren Code jedoch Fehler aufwies und gehackt wurde, wodurch DAO ein Drittel ihres Ethereum-Vermögens geraubt wurde. Über den Umgang mit diesem Fehler konnte die Community keine Einigung finden. Also wurde die Ethereum-Blockchain gespalten in eine, in der dieser Raub geschehen war, und eine, wo er nicht geschehen war. Auch bei Bitcoin selbst vollzog sich 2017 eine Blockchain-Teilung, da es einen Disput über technische Parameter gab. Es entstand die parallele Währung Bitcoin Cash.

Es zeigt sich also, dass die Historie einer Blockchain zwar technisch unveränderlich angelegt ist, jedoch die Einsatzkontexte und sozialen Bedingungen der realweltlichen Nutzung sehr großen Einfluss darauf haben, inwiefern die technisch implementierte Unveränderlichkeit tatsächlich wirksam ist. Da die Blockchain-Anwendungen in Software realisiert sind, werden Änderungen durch Code-Änderungen verursacht. Aber nicht jede Person kann Änderungen am Code vornehmen. Wie wird also entschieden, wohin sich das Netzwerk bewegt? Wenn gilt: „Code is law“, wer ist dann die „Legislative“? Und von wem werden warum welche Entscheidungen umgesetzt? Offensichtlich spielen dabei nicht technische – vielleicht sogar quasidemokratische – Verfahren zur sozialen Aushandlung, Regulierung und Konfliktlösung eine wesentliche Rolle. Genau das hatte die Blockchain jedoch ursprünglich technisch obsolet machen wollen.

Rainer Rehak



Rainer Rehak beschäftigt sich seit rund zehn Jahren mit dem Themenfeld *Informatik und Gesellschaft*. Er studierte Informatik und Philosophie in Berlin, Hong Kong und Peking. Während des Studiums arbeitete er am Lehrstuhl für *Informatik in Bildung und Gesellschaft* von Wolfgang Coy. Aktuell promoviert er am Weizenbaum-Institut für die vernetzte Gesellschaft und lehrt in den Bereichen Datenschutz/Datensicherheit sowie Informatik und Gesellschaft.

Ein weiteres, grundsätzlicheres Problem geht mit der Blockchain einher: Nehmen wir an, eine Blockchain würde tatsächlich die Eigenschaften der Unveränderlichkeit, Öffentlichkeit, Verteiltheit und damit Vertrauenslosigkeit ideal umsetzen: Wie kann nun die Richtigkeit der in der Blockchain gespeicherten Daten sichergestellt werden? Bei Finanztransaktionen ist dies vergleichsweise einfach, kann doch jeder Akteur nur das Geld ausgeben, das im eigenen Account vorhanden ist. Sobald es aber um Aussagen über die Realwelt geht, etwa ob ein Besitzgegenstand Schaden genommen hat, sodass eine Versicherung den Schaden begleichen müsste, leistet die Blockchain nur die unveränderbare Dokumentation der Behauptungen. Das Problem der Richtigkeit und Verlässlichkeit bleibt ungelöst.

Der ewige Wunsch, soziale und gesellschaftliche Probleme durch neutrale Technik lösen zu wollen, bleibt auch mit der Blockchain unerfüllbar. Sie lässt die Intermediäre nicht verschwinden, sondern verschiebt sie nur in Bereiche, die technisch nicht mehr direkt abbildbar sind. Zudem folgen die Versuche, Intermediäre aufzulösen, dem neoliberalen Mantra der Individualisierung gesellschaftlicher Risiken: Wesentliche Verantwortung liegt wieder auf den Schultern der einzelnen Person. Wehe denen, die ihr Erspartes durch einen Hack verlieren, weil der heimische Rechner und damit das Bitcoin-Portemonnaie nicht hinreichend abgesichert oder der smarte Rentenvertrag schlecht programmiert war.

Als Gesellschaft müssen wir entscheiden: Ist die Illusion, ohne vertrauenswürdige Dritte auszukommen, wirklich den massiven Ressourcenaufwand permanenter Parallelberechnung wert? Kann dieser in Technik gegossene Anti-Institutionalismus wirklich Grundlage einer Gesellschaft sein? Die Antwort auf diese Frage zeichnet sich in der Bitcoin-Blockchain ab: Das Fehlen von Machtasymmetrien ausgleichenden Institutionen mündet hier letztendlich im anarcho-libertären Recht des (Rechen-) Stärkeren. Gesellschaftliche Subsysteme sind immer vertrauensbasiert – die Frage ist nur, wie das Vertrauen ausgehandelt und legitimiert werden kann. So gesehen wäre das Bitcoin-Projekt ein gut verborgener, aber sehr nachdrücklicher Aufruf zur überfälligen Demokratisierung des Bankensystems.

Literatur

Golumbia D (2018) Zealots of the Blockchain – The True Believers of the Bitcoin Cult. In: The Baffler, 03/2018. Online: https://thebaffler.com/salvos/zealots-of-the-blockchain-golumbia (Stand 01.08.2018).

Irrera A, McCrank J (2018) Wall Street Rethinks Blockchain Projects as Euphoria Meets Reality. In: Reuters, 27.3.2018. Online: https://www.reuters.com/article/us-banks-fintech-blockchain/wall-street-rethinks-blockchain-projects-as-eupho-ria-meets-reality-idUSKBN1H32GO (Stand: 01.08.2018).

Jeffries A (2018) Blockchain Is Meaningless. In: The Verge, 7.3.2018. Online: https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethere-um-cryptocurrency-meaning (Stand 01.08.2018).

Kleintz T (2018) Missverständnisse zur Blockchain. In: Notizblog Pointers & Pointen, 1.2.2018. Online: https://notes.computernotizen.de/2018/02/01/missverstaendnisse-zur-blockchain/ (Stand 01.08.2018).

Peck ME (2017) Do You Need a Blockchain?. In: IEEE Spectrum, 29.9.2017. Online: https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain (Stand 01.08.2018).

Gerhart Baum im Interview mit Astrid Löffler

„Scheibchenweise wird Freiheit für eine fragwürdige Sicherheit geopfert“

Warum der frühere Bundesinnenminister Gerhart Baum die Menschenrechte in Gefahr sieht und welche Rolle dabei die Digitalisierung spielt

Vor 70 Jahren, im Dezember 1948, verabschiedeten die Vereinten Nationen (UN) die Allgemeine Erklärung der Menschenrechte. In ihrem 1. Artikel wird festgestellt: „Alle Menschen sind frei und gleich an Würde und Rechten geboren. Sie sind mit Vernunft und Gewissen begabt und sollen einander im Geiste der Brüderlichkeit begegnen.“ *Wir sprachen mit dem früheren Bundesinnenminister Gerhart Baum, wie es um die Umsetzung dieses Artikels heute steht, welche Chancen und Risiken dabei die Digitalisierung birgt.*

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Herr Baum, wie stehen wir in Sachen Menschenrechte heute da?

Gerhart Baum: Die Allgemeine Erklärung der Menschenrechte 1948 war ein Meilenstein in der Geschichte der Menschheit. Ein solches deutliches Bekenntnis zum Menschenrechtsschutz hat es in der Völkergemeinschaft nie zuvor gegeben. Sie war eine Reaktion auf die Barbarei des vorigen Jahrhunderts. In der Folge hat sich ein Völkerrecht entwickelt, das die Menschenrechte konkretisiert – bis heute, etwa durch die Einrichtung eines Internationalen Strafgerichtshofes. Die Täter bleiben nicht länger straflos. Das heißt, wir haben ein Instrumentarium, wir haben auch ein verändertes Bewusstsein, aber wir haben auf der ganzen Welt nicht nur Fortschritte, sondern nach wie vor schwere Verletzungen der Menschenwürde in vielen Staaten.

Wird die UN-Menschenrechtscharta denn heute überhaupt noch als Errungenschaft oder vielmehr als selbstverständlich wahrgenommen?

Baum: Das ist immer die Gefahr, dass etwas, was lange besteht, als selbstverständlich erachtet wird. Das gilt für unser Grundgesetz und auch für die Europäische Einigung. Aber ich glaube schon, dass viele Menschen begriffen haben, wie wichtig die Menschenrechte sind. Sie sind untrennbarer Teil unserer Außenpolitik. Menschenrechtsverletzungen werden deutlich am Schicksal einzelner Menschen, so im Fall des seit Monaten inhaftierten ukrainischen Journalisten Oleg Senzow, der in einem sibirischen Lager im Hungerstreik ist. Nehmen wir die Menschenrechtsverletzungen in China, und da beispielhaft die Anteilnahme an Inhaftierung und Tod des Friedensnobelpreisträ-