Kontrolle ist gut, Vertrauen ist besser, Bezahlung am besten

Zur Souveränität von Blockchains

Oliver Leistert

> Anything that can conceive of as a supply chain, blockchain can vastly improve its efficiency – it doesn't matter if it's people, numbers, data, money.
>
> — Ginni Rometty, CEO IBM

Der Werbespruch des CEO von IBM ist nicht nur vollmundig, sondern aus der Perspektive des Technologie-Giganten aus dem 20. Jahrhundert notwendig. Denn IBM spielt im Geschäft mit der *Blockchain*-Technologie global gesehen trotz großer Investitionen nur eine bescheidene Rolle. Das liegt auch daran, dass der *Blockchain*-Markt ein strukturelles Unikat ist: Als der Boom ungefähr mit Beginn der 2010er Jahre begann, waren im R&D von *Blockchains* asiatische Akteure von Anfang an sehr aktiv und mit viel Kapital dabei. China hat den Gang der Entwicklung von Anfang an stark mitgeprägt. Außerdem hat diese Sparte mit ihrer selbst erfundenen und in weiten Teilen der Welt inzwischen stark regulierten Art und Weise des Fundings, den sogenannten *Initital Coin Offerings* (ICOs), eine neue Hacker- und Start-Up-Kultur initiiert, in deren Rahmen die Finanzierung von hunderten Projekten mit Milliardensummen erfolgte.[1] Die Geburt einer libertären Fintech-Hacker-Kultur, die zwar größtenteils nicht mit dem im Kern kollaborativen Paradigma von Open Source bricht, deren monetärer Anreiz jedoch alles andere überdeterminiert, prägt das Feld mindestens genauso stark wie die Tech-Giganten aus den USA. Zusammengefasst gesagt, wird der Markt von Amazon Web Services genauso bespielt wie von Spin-offs chinesischer Technikuniversitäten, von denen außerhalb Chinas niemand gehört hatte. Dort sind allein dieses Jahr bereits 600 neue Firmen, in deren Mittelpunkt Anwendungen mit

[1] Ungefähr 22 Milliarden USD wurden bis 31.10.2018 laut Coindesk mit ICOs eingesammelt. Siehe https://www.coindesk.com/ico-tracker (05.06.2019). Herausragend ist der ICO des EOS-Blockchain-Projektes mit unglaublichen 4,2 Milliarden USD im Jahr 2018. Seit Ende des Jahres 2018 sind ICOs in vielen Ländern verboten worden.

Blockchains stehen, registiert worden.[2] Dabei fehlen dem Land einem Sprecher der International Fintech Innovation Conference zufolge 500.000 passend ausgebildete Fachkräfte.[3]

Auch hierzulande beginnt allmählich eine stärkere Integration dieser neuen Technologie. Weniger führt dies allerdings das Fraunhofer-Institut an, das für das Bundesamt für Migration und Flüchtlinge mehrere Piloten durchführt, bei denen *Blockchains* den Asylprozess optimieren sollen. Der praktische Nutzen hiervon bleibt bis heute unklar.[4] Vielleicht geht es mehr um Wirtschaftsförderung in dem von der CSU geführten Ressort und um die Fortführung einer unheimlichen Tradition, die Geflüchtete als Versuchskaninchen für neue ID-Technologien benutzt: *Eurodac*, die erste biometrische Datenbank der EU aus dem Jahre 2003, wurde zur Verwaltung von Geflüchteten in die Welt gesetzt. Und jüngst hat der Pilot einer biometrisch erfassten und per *Blockchain* abgewickelten Lebensmittelvergabe an Kriegsflüchtlinge in Jordanien für den erwünschten PR-Erfolg von Blockchains als unbestechliche Systeme in korrupten Strukturen gesorgt.[5] Die EU erprobt – eher leise – eine EU-*Blockchain*, die den Dokumententransfer zwischen zentralisiert organisierten Verwaltungen ihrer Mitgliedsstaaten dezentral leistet.[6]

In jedem Fall haben die genannten Anwendungen irritierend wenig mit libertären Digitalgeld-Fantasien zu tun, wie sie von den Fans der historisch ersten *Blockchain* vorgetragen werden. *Bitcoin* ist nach 10 Jahren und nach derzeit[7] ungefähr 220 GByte maschinisch-autonomer Kettenproduktion zu einer Industrie mutiert, die sich durch spezielle Hardware auszeichnet, am besten in direkter Nähe zu Kraftwerken steht und durch ein Rennen um die größte Rechenkraft gekennzeichnet ist.

---

2 Neben dem Terminus *Blockchain* wird oft auch der Terminus *Distributed Ledger Technologies* (*DLT*), verwendet. Beides sind m. E. passende Termini; in diesem Text wird durchgängig der Terminus *Blockchain* verwendet.

3 Bakyt Azimkanov: A Blockchain Talent Shortage in China Salls for Closer Collaboration, unter: https://cardanofoundation.org/en/news/a-blockchain-talent-shortage-in-china-calls-for-closer-collaboration/ (05.06.2019).

4 Anna Bisell: Bloß nicht verzetteln: das BAMF und seine IT-Projekte, unter: https://netzpolitik.org/2019/bloss-nicht-verzetteln-das-bamf-und-seine-it-projekte/ (05.06.2019).

5 Anna Maria Echterhölter: From Rationing Cupons to Refugee Credit: Behavioural Payment in Times of Disruption, in: Peter Pfeiffer und Nathan Tschepik (Hg.): The Meanings of Modern Work, Rochester 2018 (im Druck).

6 Christoph Bergmann: »Jedes europäische Land könnte drei oder vier Knoten haben. Vielleicht auch mehr.«, unter: https://bitcoinblog.de/2019/06/04/jedes-europaeische-land-koennte-drei-oder-vier-knoten-haben-vielleicht-auch-mehr/ (05.06.2019).

7 Für die aktuelle Länge siehe https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (02.05.2019).

Finanzprodukte traditioneller Provenienz sind weiterhin weitestgehend vom Spekulieren mit dem neuen geschürften Digital-Gold ausgeschlossen. Dafür werden Blockchains in und zwischen Banken, Finanzdienstleistern und deren Dienstleistern nicht nur intensiv getestet, sondern, glaubt man der PR, auch eingesetzt – allerdings in gänzlich anderer Bauart, als es der Emporkömmling *Bitcoin* vorgemacht hat. *Blockchains* sind hier reduziert zu einem Rationalisierungsschub zur Freisetzung von Personal, da sie bestimmte Kontrollinstanzen im Finanzfluss kryptographisch überprüfbar überschreiben. Im Prinzip sind alle Funktionsstellen des Validierens und der Authentifizierung, sei es in der Verwaltung, in der Logistik, notarieller Natur oder eben der Wertetransaktionen einer Reformatierung durch diese Medientechnologie vorgeschlagen.

Dies sind vielstimmige Schlaglichter einer inzwischen eher stillen technischen Revolution, die, typisch für solch medientechnologische Umbrüche, schon zu Beginn totgesagt wurde, als Problemlösung nicht-existierender Probleme beschrieben wird und insbesondere ihren Wahrheitsdiskurs noch nicht unter Kontrolle hat. Der historische Einsatzpunkt dieses Textes lautet insofern: Das allgemeine Phänomen *Blockchain* muss dringend analytisch seziert werden, um exemplarisch die verschiedenen Stränge von dessen Assemblagen freizulegen und deren Effekte auf bestehende Dispositive und Diskurse vorläufig und teils spekulativ zu konstatieren.[8] Die These, die hierbei diesen Text leitet, lautet, dass wir mit *Blockchains* der Entstehung einer souveränen Medientechnologie beiwohnen. Diese begriffliche medientheoretische Einordnung ist ein Vorschlag, mit dieser Technik einen theoretischen Umgang zu finden, der es gestattet, Blockchains machtanalytisch zu untersuchen, und zwar nicht nur als Kontrolltechnologien digitaler Kulturen – das ist durch die anmoderierten Beispiele hoffentlich schon plastisch geworden. Vielmehr ist der Vorschlag, *Blockchains*, oder zumindest einige Spielarten davon, als generisch digitale Souveränitäten zu begreifen, d. h. als emergente Phänomene einer environmentalen Techno-Ökologie[9], deren Souveränität sich in der Produktion von Wahrheit *und* deren maschinischer Operationalisierbarkeit zeigt. In

8 Insofern stellt er die Fortsetzung zweier Texte zum Thema dar, die sich in erster Linie mit der Warenwelt und ihrer Ausweitung und Funktionserweiterung durch Blockchains beschätigen. Siehe Oliver Leistert: Das Internet der Werte. Bitcoin und Blockchains als Boten einer verwalteten Welt 2.0, in: Phase 2 56 (Herbst 2018), S. 28–34. Siehe auch Oliver Leistert: The Blockchain as a Modulator of Existence, unter http://networkcultures.org/moneylab/2018/02/07/the-blockchain-as-a-modulator-of-existence/ (03.05.2019).

9 Zur environmentalen Techno-Ökologie siehe Erich Hörl: Die environmentalitäre Situation. Überlegungen zum Umweltlich-Werden von Denken, Macht und Kapital, in: Internationales Jahrbuch für Medienphilosophie 4/1 (2018), S. 221–250; und allgemeiner zur Frage einer nicht-natürlichen Ökologie und Technik: Erich Hörl und James Burton (Hg.): General Ecology: The New Ecological Paradigm, London 2017.

diesem Sinne verstehe ich souveräne Medientechnologien als apodiktisch, denn sie können innerhalb ihres Wahrheitsregimes nichts als die Wahrheit produzieren. Souverän heißt aber eben auch, dass sie gleichzeitig epistemisch *carte blanche* haben. Ihre Wissensoperationen sind immanent nicht anzweifelbar.

Seit knapp zehn Jahren können wir das Aufschimmern dieser neuen Formation souveräner Medientechnologien beobachten. Verteilte *Peer-to-Peer*-Netzwerke mit Protokollen zur maschinischen Konsensbildung der Fortschreibung ihrer verwalteten Kette an Datenblöcken sind seit dem Auftauchen von *Bitcoin* zahlreich und vielgestaltig.[10]

Die Versprechen und Ankündigungen, was mit *Blockchains* alles zu seinem Ende bzw. Anfang komme, waren gigantisch. Auch dies mag ein Grund sein, warum vielerorts mit Zurückhaltung oder aggressiver Ablehnung auf den Quereinsteiger *Blockchain* reagiert wurde. Mit Sicherheit ist die Verunsicherung nach wie vor groß, was eine Medientechnologie anrichten wird, die in die Welt kam, um autonom Werte bzw. Token zu verwalten.

Im folgenden Text wird es also zunächst um eine technisch-konzeptuelle Beschreibung von *Blockchains* gehen, die auf deren Besonderheiten und neue Verknüpfungen von Techniken mit dem Ziel eingeht, verständlich zu machen, warum eine Rekonfiguration von Machttechniken und -verhältnissen durch *Blockchains* angestoßen ist. Allerdings sind die Machtverhältnisse, die hier umgearbeitet werden, der Herrschaft immanent. Entgegen der beim Aufkommen neuer Medientechnologien üblichen Befreiungs- und Revolutionsrhetorik – es sei an den Beginn des Internets erinnert –, wird in Anbetracht von *Blockchain*-Technologien von einer symbiotischen Beziehung zu bestehenden Herrschaftsstrukturen ausgegangen. Insbesondere Strukturen, die von einer weiteren Deterritorialisierung von Finanzen und Verwaltung profitieren und für die eine Reterritorialisierung durch exekutierbaren Code förderlich ist, können in dezentralen souveränen Blockchains einen nach wie vor kaum abschätzbaren Rationalisierungsschub erwarten.

Diese Rekonfiguration ist ein der Kapitalbewegung korrelierendes Phänomen, durch das dessen Informations- und Wert-Operationen mittels autonomer Maschinen dem Zugriff seiner traditionellen Agenten mehr und mehr entzogen wird. Damit entsteht eine merkwürdige schillernde Entität, die die Verwaltung und Überschreibung von Werten der Manipulierbarkeit und damit schlechthin dem Zugriff nicht-systemischer Aktanten in einem bestimmten Sinne und Umfang entzieht. Anders gesagt: *Blockchains* autonomisieren Wertoperationen, indem sie Werte und allgemeine *Assets* maschinenlesbar formatiert und mit kryptographi-

10 Hier und in der Folge ist überwiegend von *bitcoin* die Rede. Die *Forks* und Varianten von *bitcoin*, die grundsätzlich auf dieselbe Art funktionieren, sind zahlreich und mitgemeint, der Lesbarkeit halber aber weggelassen.

schen Existenznachweisen versehen zu Variablen in autonomen, im Sinne von eigengesetzlichen, also souveränen *Peer-to-Peer*-Netzwerken umarbeiten. Diese Abkopplung passiert protokolllogisch auf der Ebene der eigenzeitlich getakteten Fortschreibung der Blöcke und damit Daten. Durch die Integration von Programmen, die auf diese Werte Zugriff haben und damit Operationen durchführen, den sogenannten *Smart Contracts*, entwickelt sich im Verbund dann ein weiterer Aspekt einer Souveränität, die nicht nur die Bedingungen ihrer eigene Fortschreibung in Form ihres Konsensprotokolls mitbringt, sondern zudem die Transaktionen darin selbst chronographisch kontrolliert und Zugriff auf alle Werte hat.

An dieser Stelle spätestens scheinen fundamentale Konflikte mit staatlichen Regulierern und Behörden auf, deren Rolle durch *Blockchain*-Technologien problematisiert wird.[11]

Zum besseren Verständnis des Durcheinanders geht es im Folgenden um die Blockchains in technischer Hinsicht – d. h. deren technische Bestandteile und darin insbesondere die Rolle von Konsensprotokollen. Im Anschluss an diese Bestandsaufnahme kann der Ausblick auf die originäre Mächtigkeit von Blockchains erst beginnen.

1. Die Elemente medientechnologischer Souveränität

Eine typische Blockchain besteht im automatischen Aneinanderhängen von Blöcken, die sequenziell eine Kette bilden. Die Blöcke enthalten in ihren *Headern Hash Pointer*, die jeweils auf den vorangehenden Block zeigen. Dies stellt die rückwärtige Korrektheit sicher, denn ein *Hash* ist ein mathematischer Fingerprint eines anderen, komplexeren Objekts, in diesem Fall des vorangegangenen Blocks.

Durch die sequentielle kryptographische Sicherung generiert eine *Blockchain* auch stets ihr eigenes souveränes Zeit-Regime, das die Blöcke zeitlich unfälschbar in ihren *Headern* stempelt. Die Transaktionsdaten sind im Körper des Blocks als *Hash*-Baum, auch *Merkle Tree* genannt, abgebildet, dessen *Root Hash* im *Header* zum *Hash Pointer* hinzugerechnet wird. *Merkle Trees* sind, vereinfacht gesagt, Datenstrukturen zur Sicherstellung der Integrität von Daten.

11 Für eine erste, jedoch US-zentrierte Diskussion des algorithmisch exekutierbaren Gesetzes, siehe Primavera De Filippi und Aaron Wright: Blockchain and the Law: The Rule of Code, Cambridge, MA 2018. Einen summarischen Überblick zur Relation von Souveränität und Blockchains mit vorsichtigen Einschätzungen des Zeithorizonts einer technologischen Souveränität bieten Sarah Manski und Ben Manski: No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World, in: Law and Critique 29/2 (2018), S. 151–62.

Jenseits des Aufzeichnens der Transaktionsgeschichte lassen sich in den Blöcken der meisten Blockchains zahlreiche weitere Daten speichern. Die *Bitcoin*-Blockchain enthält unzählige Einträge, die sich die Ausfallsicherheit der Kette zunutze machen. Die Spanne reicht von Grüßen, Bildern, Heiratsdokumenten und Liebesbekundungen bis zu Links auf kinderpornographische Seiten, die, da sie einer souveränen Medientechnologie aufgegeben wurden, unlöschbar sind. Darüber hinaus lassen sich aber auch Skripte unterschiedlichster Komplexitäten in der Blockchain speichern.

Eines sei an dieser Stelle angemerkt: Wenn es im Folgenden um Blockchains geht, sind nur die öffentlich einsehbare *Peer-to-Peer*-Netzwerke gemeint, die durch ein Protokoll zur Konsensbildung darüber, was gegenwärtig der Fall ist, und im Takt des Protokolls zur Akzeptanz der Vergangenheit regiert werden. In diese Netze können sich jederzeit Knoten ein- und aushängen, ohne dafür um Erlaubnis fragen (*permissionless*) und ohne sich ausweisen zu müssen. Die Knoten dieser Ketten propagieren ihre Information über *Gossiping*, d. h. von Knoten zu Knoten in nachbarschaftlicher Topologie.[12] Nur in diesem Setting wird der hier konzeptuell vorgeschlagene Tatbestand der medientechnologischen Souveränität erfüllt. In diesem Setting ist es unerheblich, wer die Knoten betreibt und – bis zu einer bestimmten tolerierbaren Grenze – ob die Knoten vom Protokoll abweichende und darum bösartige Absichten verfolgen, die protokolllogisch wiederum zu bestrafen sind (keine Belohnungen bis hin zum automatischen Abschalten, je nach Protokoll). In diesem Setting sind am Netzwerk teilnehmende Knoten dynamisch zu- und abschaltbare Elemente einer verteilten Souveränität protokolllogischer Konsens-, Wahrheits- oder Existenzfindung.[13]

Im *Peer-to-Peer*-Netzwerk gibt es keine zentrale Instanz, die das Netzwerk verwaltet oder eine besondere Position darin einnimmt.[14] Auch gibt es keine zentrale

12 Im Text wird dezentral und verteilt synonym verwendet. Zum Mythos und der Realität von Dezentralität im Blockchain-Diskurs siehe Balazs Bodó und Alexandra Giannopoulou: The Logics of Technology Decentralization: the Case of Distributed Ledger Technologies, in: Massimo Ragnedda und Giuseppe Destefanis (Hg.): Blockchain and Web 3.0: Social, Economic, and Technological Challenges, New York 2019 (im Druck). Zu verteilten Netzen und deren Topologien als politische Strukturen siehe Oliver Leistert: Individuation, Nachbarschaft und Protokoll – Spontane Routen-Emergenz in Meshnetzwerken, in: Maik Bierwirth, Oliver Leistert und Renate Wieser (Hg.): Ungeplante Strukturen: Tausch und Zirkulation, München 2010, S. 33–46.

13 Kurz erwähnt werden sollen an dieser Stelle andere Settings, die auch unter dem Label Blockchain laufen. Insbesondere nicht öffentliche, zulassungsbeschränkte Blockchains (*permissioned*), wie solche auf Basis von *Hyperledger Fabric*, das von einem Industrie-Konsortium unter dem Dach der *Linux-Foundation* entwickelt wird und das z. B. von *Amazon Web Service* als zubuchbare Option des Business-Cloudpakets angeboten wird, folgen gänzlich anderen Logiken und werden in diesem Text nicht behandelt.

14 Es gibt eine lange Vorgeschichte dieses Technologieverbunds, die hier nicht referiert

Autorität. Alle Knoten sind gleichrangig und -förmig für dessen Betrieb verantwortlich. *Peers* sind *Server* und *Client* zugleich. Sie validieren Transaktionen und stellen sie fertig, genauso wie sie welche in Auftrag geben. Das Konsensprotokoll hat die Aufgabe, sicherzustellen, dass jeder Knoten im Netz den Inhalt und die Reihenfolge der Transaktionen der bestätigten *Blockchain*-Struktur übernimmt, dass jeder Knoten, wenn ein neuer *Block Header* bestätigt wurde, seine lokale *Blockchain*-Struktur aktualisiert, und dass alle Transaktionen auf ihren Konsens hin rückwärts überprüft werden können. Diese drei Eigenschaften eines Konsensprotokolls heißen Korrektheit, Konsistenz und Rückverfolgbarkeit. Im öffentlichen und auf alle Knoten verteilten Buchungsbuch, dem *Ledger*, sind alle Transaktionen aller Zeiten vermerkt.

Dieses Modell eines Verzichts auf eine zentrale Autorität und auf Zugangskontrolle wird im Englischen *trustless* genannt, was nur schlecht mit ›ohne Vertrauen‹ übersetzbar ist. Gemeint ist nicht, dass kein Knoten im Netz einem anderen Knoten vertraut, sondern dass ein Konsensprotokoll in alle Knoten Regeln implementiert, anhand derer operativ von allen Knoten verteilt und automatisch Konsens im Zuge der Teilnahme am Netzwerk hergestellt wird. Es läßt sich insofern als *ein sich individuierendes Netzwerk beschreiben, das unter rein immanenten Bedingungen seine eigene wahrhaftige Fortschreibung durchführt*. Keine dritte, äußere Instanz vermag den Gang der Entwicklung zu beeinflussen. Diese immanenten Bedingungen sind zum Start des Netzwerkes protokolllogisch festgelegt, und eine Änderung von außen erfüllt den Tatbestand der Transzendenz, der unbedingt vermieden werden muss, damit die Souveränität, die sich aus sich selbst heraus in die Zukunft hinein schreibt, bestehen bleibt. *Blockchain*-Souveränität ist zutiefst anti-transzendent.

Es kam und kommt in der Geschichte von *Blockchains* zu Protokoll-Updates. Diese sind zu unterscheiden in solche, die die Rückwärtskompatibilität mit der *Blockchain* erhalten, und jene, die das nicht können und einen *Fork* einleiten müs-

---

wird. Die Informatik beschäftigt, wie in verteilten Systemen die richtige Reihenfolge von Computationen stattfinden kann und in der Folge wie solche Systeme zu synchronisieren sind. Siehe hierzu die Arbeiten von Leslie Lamport zur Uhrsynchronisation in verteilten Systemen: Leslie Lamport, Robert Shostak und Marshall Pease: The Byzantine Generals Problem, in: ACM Transactions on Programming Languages and Systems 4/3 (1982), S. 382–401. Ferner ist die Frage, wie ein nur teilweise synchrones Netzwerk konsensual arbeiten kann, zu erforschen gewesen. Siehe hierzu Cynthia Dwork, Nancy Lynch und Larry Stockmeyer: Consensus in the Presence of Partial Synchrony, in: Journal of the ACM 35/2 (1988), S. 288–323. Auch sind in die Entwicklung von Ad-hoc-Netzwerken Forschungen zur Konsensbildung für asynchrone Netzwerke eingegangen. Hervorzuheben sind hier probabilistische Ansätze zur Terminierung von Computationen und die Einbeziehung von Zufall in die Regeln des Betriebs. Siehe Gabriel Bracha und Sam Toueg: Asynchronous Consensus and Broadcast Protocols, in: Journal of the ACM 32/4 (1985), S. 824–40.

sen. Ein unlösbarer Streit unter Entwickler*innen-Teams über solch ein Update führte bereits zu spektakulären *Forks*. Am 1. August 2017 *forkte* eine Gruppe von Entwickler*innen die *Bitcoin-Blockchain* und es entstand *Bitcoin Cash*, das pro Block mehr Speicherplatz hat als *Bitcoin*. Doch damit nicht genug. Als Resultat eines veritablen Bürgerkrieges zweier Fraktionen im *Bitcoin Cash*-Lager erfolgte erneut ein harter *Fork*, der sich abermals an der Frage der Größe der Blöcke entspannte. Aus Sicht souveräner Medientechnologien sind diese Momente zu vermeiden und müssen als vorgeschichtliche Störungen der environmentalen Souveränitätsemergenz gelten.[15]

Es gibt jedoch auch protokolllogisch antizipierte Momente des Dissenses im Netzwerk. Nicht alle lokalen *Blockchain*-Sätze aller dezentralen Knoten können synchron die Wahrheit aktualisieren bzw. von ihr aktualisiert werden. Der Konsens über die gültige Reihenfolge und den gültigen Inhalt ist immer auch irgendwo im Netz gebrochen, und immer existieren mehrere Vorschläge einer errechneten Wahrheit. Für diese Wahrheitsunschärfe hat ein Konsensprotokoll zunächst die einfache Regel vorgesehen, dass stets die längste Kette die wahre Kette ist bzw. den Konsens bildet. Dennoch können Devianzen auftreten, die sich in *Forks*, d. h. neuen Ketten, die eine neue Realität behaupten und sich gabeln, ausdrücken. Häufig ist in partiell synchronen *Peer-to-Peer*-Netzwerken von *Blockchains* eine Fehlertoleranz von 49% gegeben. Die Mehrheit der teilnehmenden Knoten muss für ein zuverlässiges Funktionieren der Technologie den Konsens bilden. Der Rest kann, sogar gemeinsam, an einer anderen Kette bauen – geht dann aber in der Folge leer aus. Es gilt hier die Regel, dass möglichst wenig Knoten falsche neue Enden bauen, da damit unnötig Rechenkapazität verbraucht wird und Knoten, die in Parallelwahrheiten unterwegs sind, das Netzwerk nicht mehr unterstützen.[16] Um zu vermeiden, dass eine kürzere Kette von anderen Knoten als Wahrheit akzeptiert wird, sorgt das Konsensprotokoll dafür, dass z. B. ein finanzieller Verlust für den Knoten entsteht, der nicht auf die längste Kette baut, sondern einem alternativen *Fork* folgt.

15 Zum Eingriff in das Regierungsprotokoll von *Ethereum* und dem folgenden Fork in *Ethereum* und *Ethereum Classic*, siehe Quinn DuPont: Experiments in Algorithmic Governance: A History and Ethnography of »The DAO«, a Failed Decentralized Autonomous Organization, in: Malcolm Campbell-Verduyn (Hg.): Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance, New York 2018, S. 157–177.

16 Unter https://www.blockchain.com/btc/orphaned-blocks (05.06.2019) lassen sich alle Parallelwelten von *bitcoin* nachschlagen.

2. Das Nakamoto-Konsensprotokoll und andere

Das unter den Konsensprotokollen bekannteste ist das in *Bitcoin* implementierte arbeitsbeweisbasierte Nakamoto-Konsensprotokoll, das abgewandelt auch z. B. in *Litecoin* oder *Ethereum* zur Anwendung kommt. Die Idee des arbeitsintensiven Rechenbeweises ist übrigens durchaus schlau: Da das *bitcoin*-Netzwerk öffentlich und der Aufwand sehr gering ist, als Knoten mit einer Vielzahl von Identitäten und Adressen aufzuwarten, die dann den Konsens mitbestimmen würden, wird einer solchen sogenannte *Sybil*-Attacke begegnet, indem alle, die am Konsens mitwirken wollen, um bei Erfolg mit neuen *Bitcoins* belohnt zu werden, arbeiten, also schuften müssen. Solch ein Schuften realisiert sich im *Bitcoin*-Netzwerk über Investitionen in Hardware, die nichts anderes macht, als auf der Suche nach dem richtigen *Hash* Rechenkraft zu verbraten. Dieses Protokoll erreicht seinen Konsens über das Lösen eines mathematischen Puzzles. Es muss ein *Hash*-Wert gefunden werden, der bestimmte Kriterien erfüllt. Damit der Takt der Blockerzeugung (alle 10 Minuten) ungefähr gleich bleibt, d. h., damit sichergestellt ist, dass der neue Block an alle *peers* im eher langsamen Netzwerk propagiert werden kann, wird die Schwierigkeit der Rechenaufgabe variiert. Wird die Speichergröße der Blocks erhöht, damit mehr Transaktionen darin Platz finden können, dauert wiederum deren Propagation im Netzwerk länger, was schnell zu nicht mehr ausreichender Verteilung der neuen Knoten als neues Ende der Kette führen kann.

Der erste Knoten, dem dies gelingt, sendet den verifizierten neuen Block zum gesamten Netzwerk, erhält die Belohnung und sammelt alle Transaktionsgebühren ein. Dieser Prozess wird *mining* genannt und wird durch Kryptographie gesichert und durch Spieltheorie modelliert. Im Kern von öffentlich zugänglichen Blockchains auf Basis von *Peer-to-Peer*-Netzwerk-Topologien ist das Protokoll der Konsensbildung unter den Knoten eine formale Implementierung von Regeln, unter denen sich alle Knoten versammeln müssen, um in den Genuss der Belohnung zu kommen.

Diese Regeln sind formalisiert in der Spieltheorie wiederzufinden, und dieses mathematische Feld, das von John von Neumann und Oskar Morgenstern kanonisiert wurde[17], hat inzwischen eine Vielzahl von Szenarien berechenbar gemacht, die realweltliches Verhalten rationaler Teilnehmer und deren Strategien abbilden. Indem Strategien und Interaktionen zwischen den Netzwerkknoten modelliert werden, können Gleichgewichte des Systems erreicht werden, die den robusten Fortbestand des Rennens um die Belohnungen und damit des Netzwerks gewährleisten.

17 John von Neumann und Oskar Morgenstern: Theory of Games and Economic Behavior (1944), Princeton 2007.

Das Sonderbare dieser Technologie ist, dass durchgängig um den Zustand der Gegenwart gerungen wird. Die Vergangenheit hingegen, ist sie einmal festgelegt, ist unveränderbar und homolog für alle Knoten. Dies ist bei gewöhnlichen Datenbanktechniken anders. Zwar können Einträge gegen ein Überschreiben kryptographisch geschützt sein, aber es ist technisch stets vorgesehen, dass ältere Einträge modifiziert werden können. Ein reines Anhängen von Daten, wie eine unendliche Folge von Perlen auf einer Kette, scheint vielmehr der Logik eines streng chronologischen Logbuchs zu folgen.

Zu erwähnen ist auch noch, dass im Nakamoto-Konsens nicht deterministisch, sondern probabilistisch gearbeitet wird, da Knoten beliebig wieder verschwinden können und niemals Synchronität herrscht. Dies bedeutet, dass akzeptierte Blöcke *niemals absolut korrekt* sind, aber dass die Wahrscheinlichkeit, dass sie falsche Blöcke sind, exponentiell schwindet.

Die Konsensbildung wird in der gegenwärtigen Forschung an Blockchains vielleicht am intensivsten weiterentwickelt. Insbesondere gilt es, die arbeitsbeweisbasierte Methode der Konsensbildung zu überwinden. Schließlich ist es schwer zu vermitteln, wieso für eine Transaktion der Stromverbrauch eines Tages von 15 US-Haushalten benötigt wird.[18]

Proof of Stake (*PoS*)-basierte Konsensprotokolle gehören zu den vorgeschlagenen Regierungsformen zukünftiger bzw. im Testbetrieb schon heutiger Blockchains. Sie benötigen wenig Rechenkraft und können den Energieverbrauch wieder auf vermittelbare Größen reduzieren. Im Zentrum dieses und anderer vorgeschlagener Verfahrens stehen weiterhin kryptographische Methoden zur Herstellung des Konsenses zwischen den Netzwerkknoten sowie die Verteilung angemessener Belohnungen an ehrliche Knoten für das konsensuale Festlegen neuer Blöcke. Kernaufgaben beinhalten nach wie vor das Finden einer Übereinkunft aller ehrlichen Knoten in Bezug auf alle Transaktionen in allen Blöcken und deren sequentieller Nummer und Akzeptanz für alle Knoten sowie deren Integrität.

Ein *Stake* bezeichnet die Tokens einer Beteiligten, die in den Prozess der Konsensbildung investiert werden. Die Chance, einen neuen Block in der Kette zu bestimmen, ist nun nicht mehr proportional zur Rechenkraft, sondern zum Wert der Einlage (*Stake*). Von den verschiedenen Varianten eines *Proof-of-Stake* Konsenses[19] sollen hier exemplarisch der *Committee-based PoS* kurz erläutert werden.

---

18 Siehe den Index des Stromverbrauchs von bitcoin unter https://digiconomist.net/bitcoin-energy-consumption (04.06.2019).

19 Für einen Überblick siehe Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn und George Danezis: Consensus in the Age of Blockchains (2017), unter: http://arxiv.org/abs/1711.03936 (04.06.2019).

Dieses Protokoll legt ein sogenanntes Komitee von Stakeholdern auf der Grundlage ihrer Einlagen fest, das berechtigt ist, in geordneter Folge neue Blöcke der Kette zu generieren. Um ein Komitee im verteilten Netzwerk festzulegen, wird ein MPC-Verfahren (*secure multiparty computation*) angewendet. Eine überprüfbare Zufallsfunktion nimmt als Input den aktuellen Zustand der Blockchain und die Einlagenwerte aller Stakeholders und gibt eine zufällige Folge von Stakeholdern aus, die nacheinander das Komitee besetzen. In dieser kryptographischen Rechnung beginnen die Teilnehmenden mit individuellen Inputs und erzeugen gemeinsam einen gleichen Output, die Sequenz der *Leader*, die das Komitee besetzen, ohne die Inputs der anderen Teilnehmenden zu kennen. Je mehr Einlagen eine Stakeholderin hat, umso mehr Stellen in der Sequenz kann sie einnehmen. Wenn also im arbeitsbeweisbasierten Verfahren diejenige die besten Chancen hat, die am meisten *Hashes* pro Sekunde durchrechnen kann, so verschiebt das *PoS* Verfahren die besten Chancen zu derjenigen im Netzwerk, die am meisten Einlagen ins Verfahren gibt. Da die mögliche Höhe der Einlagen abhängig von der Höhe des Besitzes ist, handelt es sich bei diesem Verfahren um eine *probabilistische Plutokratie*. Beispiele für dieses Regierungsprotokoll, das im Detail komplizierter ist, sind die *Ouroboros*-[20] und *Ouroboros-Praos*-[21]Protokolle von *Cardano*, aber auch die jüngst von Facebook präsentierte Digitalwährung Libra basiert technisch auf einem PoS Verfahren – allerdings wird sie in den ersten Jahren nicht *permissionless* sein.[22]

Bevor es zur weiteren machtanalytischen Einschätzung der *Blockchain*-Technologien kommt, bzw. einer Präzisierung der Rede von souveränen Medientechnologien, wird noch kurz auf die bereits erwähnten spieltheoretischen Modellierungen, die in allen *Blockchain*-Algorithmen zu finden sind, eingegangen. Sie sind wesentlicher Garant für die Stabilität der Systeme, die, daran sei erinnert, völlig transparent, ohne Regulierung von oben oder außen und zugänglich für alle, d. h. auch für Teilnehmende mit zerstörerischen oder kriminellen Absichten, eine Verwaltung von Werten betreiben.

Aus diesem Grund ist in ihren Modellen soziales (Fehl-)Verhalten modelliert und formalisiert. Wenn auf Basis dieser Modelle *Blockchains* laufen, wenn diese Systeme gegen diese Modelle getestet werden, dann ist es naheliegend, auch die

20 Aggelos Kiayias, Alexander Russell, Bernardo David und Roman Oliynykov: Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol (2016), unter: http://eprint.iacr.org/2016/889 (04.06.2019).

21 Bernardo David, Peter Gaži, Aggelos Kiayias und Alexander Russell: Ouroboros Praos: An Adaptively-secure, Semi-synchronous Proof-of-stake Protocol (2017), unter: https://eprint.iacr.org/2017/573 (04.06.2019).

22 Siehe die Sektion des Whitepapers unter: https://libra.org/en-US/permissionless-blockchain/ (16.08.2019).

durch diese Modelle replizierten und operationalisierten sozialen Beziehungen in den Blick einer Machtanalytik zu nehmen.

Spieltheorien finden in Blockchains auf unterschiedlichen Ebenen ihre Anwendung. Einerseits werden sie benutzt, um die Netzwerkknoten mittels des Konsensprotokolls zu stabilisieren, um sie in einem Gleichgewicht zu halten. Teilnehmende werden, das ist Prämisse, als rational modelliert. Dies bedeutet hier, dass sie ausschließlich am eigenen Wohlergehen bzw. Benefit interessiert sind. Akteure versuchen strategisch, ihre Gewinne zu erhöhen.[23] Alle Verfahren der Belohnung gründen auf spieltheoretischen Modellen, die dafür sorgen, dass es die dem Knoten nützlichere Entscheidung ist, nach den wahren neuen Blöcken zu suchen, als einen falschen vorzuschlagen.

In ihrer Übersicht spieltheoretischer Modellierungen von dezentralen Blockchains zeigen Liu u. a. ein breites Spektrum von Szenarien für *Blockchains* auf, die spieltheoretisch überprüft wurden.[24] In den meisten Fällen geht es um die Sicherheit des Systems. Das vielleicht bekannteste Szenario der Spieltheorie, das Nash-Equilibrium[25], sticht hervor. Benannt nach seinem Nobelpreis dotierten Erfinder John Nash, der in später Selbstauskunft angibt, stets unter paranoiden Zuständen gelitten zu haben, ergibt sich das gewünschte Equilibrium dann und genau dann, wenn ohne Strategiewechsel alle Knoten den größten statistischen Nutzen davon haben, dem Konsensprotokoll zu folgen.

Im Falle von *Bitcoin* ist es übrigens nicht eindeutig, ob dies erfüllt ist. Bekannt sind Verhalten, in denen Knoten, die als erstes einen neuen korrekten Block errechnet haben, diesen Block geheim halten und sich damit einen Vorteil gegenüber den anderen Knoten verschaffen, die weiterhin nach diesem Block suchen, während der Knoten, der den richtigen Block schon gefunden hat, bereits den nächsten suchen kann.[26] Da sich in der Realität Knoten, die nach neuen Blöcken schürfen, zu *pools* zusammenfinden, um gemeinsam eine größere Rechenkraft und damit eine höhere Wahrscheinlichkeit auf das Errechnen der neuen Spitze der Kette zu haben, gibt es in diesem *selfish mining* genannten Szenario eine Vielzahl von Interaktionen zwischen den Knoten. Auch dieses Szenario läßt sich spielthe-

23 Beniger fasst die Entwicklung von Entscheidungstheorien zu Spieltheorien kurz und präzise zusammen. James R. Beniger: The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge 1986, S. 51 ff.

24 Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang und Dong In Kim: A Survey on Blockchain: A Game Theoretical Perspective, in: IEEE Access 7 (2019), S. 47615–47643.

25 John Nash: Non-cooperative Games, in: Annals of Mathematics 54 (1951), S. 286–295.

26 Ittay Eyal und Emin Gün Sirer: Majority Is Not Enough: Bitcoin Mining Is Vulnerable, in: Nicolas Christin und Reihaneh Safavi-Naini (Hg.): Financial Cryptography and Data Security, Lecture Notes in Computer Science, Berlin/Heidelberg 2014, S. 436–54.

oretisch als nicht-kooperativ modellieren, und es läßt sich zeigen, dass tatsächlich ein Vorteil für einen *pool* entsteht, wenn er sich derart fehlverhält.[27]

Das Rennen um die Belohnung zeichnet praktisch alle Konsensprotokolle aus. Es werden i.d.R. Tokens des Systems an die Gewinner der Verfahren verteilt, die für die Fortschreibung der Ketten in ordentlicher Weise sorgen. Dies ist bei *Bitcoin* das berühmt-berüchtige *mining*, während andere Systeme, z. B. Cardano, mit einer fixen Zahl an Token von vornherein gestartet sind. Hierfür hat sich der widersprüchliche Begriff *pre-mined* etabliert. In jedem Fall aber, und dies führt zum letzten Punkt, kann ein System, das offen und dezentral läuft und einen Konsens sucht, auf Monetarisierung und ökonomistische Axiome, die überwiegend aus dem neoklassischen Mainstream der Ökonomie stammen, nicht verzichten. Projekte, die ein *Blockchain*-Netzwerk auf der Basis solidarischen Handelns betreiben, z. B. im Sinne einer Kooperative, bei der immer alle Knoten vom Konsens profitieren, sind nicht *permissionless*.[28]

Spieltheorie, dies sei zum Abschluss dieses Teils noch gesagt, spielt auch, gewissermaßen ganz klassisch, jenseits der Protokolle bei der Modellierung sogenannter *Smart Contracts* eine wichtige Rolle. Da *Smart Contracts* Regeln aufstellen, nach denen Werte in bestimmten Zeitlichkeiten auf der Blockchain verschoben werden, ähnelt das Verfahren Anwendungen in der etablierten Ökonomie, die sich spieltheoretischer Modellierungen bedient, z. B. Preistheorien, die ein Modell von Gleichgewichten benutzen.[29] Es wird hier nicht weiter auf dieses Feld eingegangen. Dass *Smart Contracts* jedoch mächtig sind, kann auch gezeigt werden, ohne einen längeren Exkurs zur Implementierung und Modellierung zu führen. Es sei hierfür vor allem an eine Grundproblematik liberaler wie auch illiberaler Vergesellschaftung erinnert: die Unmöglichkeit des Vertrauens untereinander.

---

27 Ittay Eyal: The Miner's Dilemma, in: IEEE Symposium on Security and Privacy (2015), S. 89–103.

28 Zu nennen wäre als Beispiel https://fair-coin.org/. Das Thema einer anderen Ökonomie, die mittels Blockchains realisiert werden kann, ist leider allzu oft mit einer verkürzten Kapitalismuskritik versetzt, die dem Geld wertschaffende Funktion zuschreibt. Es wäre vielmehr wichtig, den Wertbegriff als solchen zu öffnen und die Rolle des universalen Tauschäquivalents in Frage zu stellen: Was wäre ein qualitativer Wertbegriff? Siehe hierzu Oliver Leistert: On the Question of Blockchain Activism, in: Graham Meikle (Hg.): The Routledge Companion to Media and Activism, New York 2018, S. 376–384.

29 Roger B. Myerson: Game Theory: Analysis of Conflict, Cambridge, MA 1991.

3. Bezahltes Vertrauen kryptographisch kontrolliert

Bürgerliche Gesellschaften sind Gesellschaften des Vertragswesens. Es gibt keine Transaktion, die nicht vertraglich geregelt ist.[30] Insofern formalisiert und operationalisiert die *Blockchain*-Technologie ein Menschenbild, das seit Adam Smiths *Wealth of Nations* als Basis von Sozialität in die bürgerliche Ökonomie eingeschrieben ist, aber bisher keine technologische Souveränität genossen hat. *Blockchains* etablieren ein formalisiertes Vertragswesen, in der es nicht mehr den Platzhalter des Vertrauens braucht, da dieses Problem bürgerlicher Vergesellschaftung nun in Maschinen ausgelagert ist. Aus diesem Grunde ergibt sich auch ein spannungsreiches und schwieriges Verhältnis zum bürgerlichen Staat und seinen juridischen Sphären, sind sie doch darauf angewiesen, als einzige über das Einhalten von Verträgen zu wachen und zu sanktionieren. Jede *Blockchain*, die dezentral und offen mit einem Konsensprotokoll regiert wird, ist ein Mini-Paralleluniversum zur staatlichen Souveränität – es handelt sich schließlich nicht um Spiele, auch wenn dies durch den Exkurs zur Spieltheorie vielleicht anklang, sondern um Tokens, die auch immer in *Fiat*-Geld getauscht werden können. Darüberhinaus ist die Unmöglichkeit, Daten aus der Kette zu löschen, ein ins Material geschriebener Affront gegenüber Behörden und Staatsanwaltschaften.

Insofern sind es kleine souveräne Maschinenverbünde, die sich dem staatlichen Monopol auf Rechtsprechung widersetzen und alternative Verfahren der Einigung nicht nur aufweisen, sondern automatisiert exekutieren. Etwas polemisch ausgedrückt läßt sich sagen, dass *Blockchains* neue, von der Digitalisierung noch unberührte Elemente des bürgerlichen Betriebssystems durch und durch maschinenlesbar gemacht haben. In der Welt der symbolverarbeitenden Maschinen einmal angekommen, dies zeigen alle Rationalisierungsschritte und -entwicklungen, gibt es keinen Weg mehr zurück ins Manuelle. Deshalb sind *Blockchains* so anziehend und gefährlich zugleich. Denn es stellt sich zurecht die Frage, wieso diese Technologie einen unerhörten Investitionsboom in der IT-Branche in Form unzähliger Start-ups auslösen konnte. Aus gesellschaftskritischer Perspektive bieten sich aber durchaus Erklärungen des Phänomens jenseits eines kollektiven Fiebers an. Schließlich lösen *Blockchains* ein uraltes Problem bürgerlicher Vergesellschaftung, das bis heute sehr kostenintensiv geblieben ist: das Problem des Vertrauens in einer Welt voller Feinde. Wie oben beschrieben, ist der Begriff des Vertrauens bzw. dessen Abwesenheit stets bezogen auf die dritte Partei, die vermittelt. *Blockchain*-Technologien entledigen sich mindestens auf der Ebene des Operativen einer zu vertrauenden Instanz, die traditionell eine Institution des Staates ist. Gern wird

30 Vielleicht bilden Geschenke, Almosen und Spenden Ausnahmen. Schon die Ehe ist keine mehr.

gesagt, dass *Blockchains* auf Probleme antworten, die es nicht gibt. Doch dies ist nur dann der Fall, wenn der Bezugsrahmen der Problemgröße im Rahmen der bürgerlichen Vergesellschaftung bleibt. Kritisch betrachtet ist das Problem, das Blockchains angetreten sind zu lösen, eine immanente und eben nicht revolutionäre Lösung des Problems der (il)liberalen Vergesellschaftung. Anstatt neue Formen der Relationen zu instituieren, die wirklich andere gesellschaftliche Verhältnisse zur Folge hätten – wie es solidarische Konzepte vorschlagen –, löst die Blockchain das Problem einmal mehr nur von innen: Durch eine noch tiefere Algorithmisierung souveräner Mechanismen deterritorialisiert sich die bürgerliche Eigentums- und Werte-Axiomatik, um sich mit von Rechnern erzeugten Tokens, die einfach nur blanke Identitätsnachweise von sich selbst sind, zu reterritorialisieren.

Das Problem, auf das Blockchains antworten, ist insofern eines, das mindestens ins 17. Jh. zurückreicht und mit den bürgerlichen Revolutionen erschien, d. h. das Problem politischer, aber nicht ökonomischer Gleichheit. Blockchains bleiben, das hoffe ich gezeigt zu haben, in diesem Sinne Lösungen falscher Probleme. Denn, um mit dem französischen Technik- und Individuationsphilosophen Gilbert Simondon zu enden, »ein Problem zu lösen, heißt, über es hinwegzuspringen, heißt, eine Umprägung der Formen vorzunehmen, die selbst die Vorgaben und Daten des Problems sind.«[31] Blockchains prägen keine Formen um, z. B. durch eine andere Definition von Wert, sondern prägen die Formen nur noch tiefer in den gesellschaftlichen Grund ein. Diese neuen Souveränitäten, die aus rechtslibertärer Sicht als Antipoden des Staates gedeutet werden, sind weder dessen Aufhebung noch dessen Untergang, sondern dessen Verbund-Upgrade zur algorithmischen Automatisierung gesellschaftlichen Verkehrs.

31 Gilbert Simondon: Die Existenzweise technischer Objekte, Zürich 2012, S. 132.