

benötigen«. ¹⁷ Eine institutionelle Einbindung medialer Praktiken, die auf der Basis einer dezidiert anti-institutionalistischen Technik entstehen, wäre zwar mit dem ursprünglich (krypto-)anarchistischen Geist der *Blockchain* kaum vereinbar, aber machte sie möglicherweise deutlich demokratie-kompatibler. Vielleicht gilt es der Freiheit, welche die *Blockchain* verspricht, nicht weniger, sondern mehr (und andere) ›Ketten‹ anzulegen, damit sie werden kann, was sie sein soll.

¹⁷ Yochai Benkler: Degree of Freedom, Dimensions of Power, in: *Daedalus, the Journal of the American Academy of Arts & Science*, 145/18 (2016), S. 30.

Ketten des (Miss-)Vertrauens

Über die Blockchain, Bitcoins und Verwandtes

Jan Claas van Treeck

1. Schichten der Repräsentation

Ich stehe in der Schlange an einer Supermarktkasse, an der sich die banalen Kleindramen einer digitalisierten Wirtschaft zeigen. Mit ruhiger Hand zieht ein Supermarktangestellter Ware um Ware, sei es nun eine Dose geschälter Tomaten, ein Becher Joghurt oder eine Tafel Schokolade, über den optischen Scanner, der die EAN-Codes der Waren erfasst – eine *pattern recognition* der basalsten Sorte. Am spannendsten in diesem Ballett der Waren ist stets Obst, das der Kunde noch selbst abwiegen muss. Die Waage druckt bekannterweise einen kleinen EAN-Code-Sticker aus, den man selbst auf seine Zucchini oder Bananen kleben muss. Hier muss die Verbindung zwischen Ware und Code also noch selbst vom Kunden durch Aufkleben hergestellt werden – man wird an das Lacan-Bonmot erinnert, wonach das Symbolische an das Reale eben nur »angeleimt« ist.¹

Aber Lacan wäre hier ein halbfauler Gesprächspartner. Das »Symbolische«, das er 1955 im Kopf hatte, war natürlich die menschliche Sprache, die er zwar bereits kybernetischen Mechanismen nahe sah, die aber weit von den EAN-Codes unseres Beispiels entfernt ist.

Lacan müsste hier mit einem Argument von Sybille Krämer verschaltet und dann weiter prozessiert werden. Laut Krämer leben wir wie selbstverständlich in einer »Zwei-Welten-Ontologie« der Repräsentation.² Über das Materielle der Dinge stülpt sich die Welt unserer Repräsentation nach dem Type-Token-Modell. Unter hochtechnischen, mithin planetarisch-digitalen Verhältnissen hat sich aber längst eine dritte Welt oder Schicht zusätzlich aufgetürmt – die der digitaltauglichen weiteren Repräsentation, ebenfalls nach dem Type-Token-Modell.

¹ Jacques Lacan: Psychoanalyse und Kybernetik. Oder von der Natur der Sprache, in: ders.: Das Seminar von Jacques Lacan. Buch II (1954–1955). Das Ich in der Theorie Freuds und der Psychoanalyse, Weinheim/Berlin 1991, S. 373–390, hier S. 381.

² Sybille Krämer: Sprache – Stimme – Schrift: Sieben Gedanken über Performativität als Medialität, in: Uwe Wirth (Hg.): Performanz. Zwischen Sprachphilosophie und Kulturwissenschaften, Frankfurt am Main 2002, S. 323–346, hier S. 323 f.

Für den Supermarktangestellten und die Kunden ist das grüne Ding eine Zucchini, und man könnte sich nun trefflich darüber streiten, was eine Zucchini ausmacht oder warum eine kleinere Zucchini denn bitte genau dasselbe kosten soll wie eine größere, wenn sich der Preis an der Supermarktkasse nach Stück und nicht nach Gewicht berechnet. Und dann gäbe es vielleicht noch den Fall eines Kindes, dessen Gemüsekompetenz noch nicht voll entwickelt ist und das grüne Ding für eine Gurke halten könnte. De Saussure lässt grüßen; Sprache ist arbiträr; wir wissen es.

Der EAN-Scanner jedoch lässt nicht mit sich diskutieren. Der gescannte Code bedeutet, dass ein Preis aus einer Datenbank abgerufen wird und eine Zucchini – was auch immer das dann realiter bedeutet – aus dem Bestand des Supermarktes entfernt wird. Der Computer, der hinter diesem System steht, operiert, er performiert nicht. Das Einscannen eines Codes steht eineindeutig für genau eine ›Zucchini‹. Hätte nun ein spaßvogeliger Kunde auf der Warentaste beim Gemüse jedoch die Taste für Bananen gedrückt, so würde eine ›Banane‹ statt der realen Zucchini gescannt, berechnet und ausgebucht. Wieder mit Lacan wird also auch diese weitere Schicht, die der operativen Verdattung der ersten Welt, genauso ›angeleimt‹ wie das Symbolische der Sprache. Und sowohl das Symbolische der Sprache als auch das operative Symbolische der Verdattung können abgelöst und ›umgeleimt‹ werden, nicht nur in der Gemüseabteilung. Leih man sich etwa in einer großen Universitätsbibliothek ein Buch aus, bemerkt man den dicken, erhabenen Aufkleber hinten im Bibliotheksbuch, unter dem sich ein RFID-Chip befindet. Für das System der Bibliothek ist nun das Buch dieser Chip – mit dem Erfolg, dass man für einen geplanten Buchdiebstahl einfach nur vorsichtig den Chipaufkleber aus dem Buch lösen – ›ableimen‹ – muss, um das Buch federnden Schrittes durch die RFID-Kontrollbaken der Bibliothek zu tragen. Für das System der Bibliothek hat das Buch die Bibliothek nicht verlassen, während der Dieb mit dem materiellen Buch das Weite sucht.

2. »Bitcoin & Crypto will change EVERYTHING«

Und es war in der Tat bei solchen Gedanken in einer langen Supermarktschlange, als ein zur Überbrückung der Kassenschlangenlangeweile getaner kurzer Check meines Twitter-Accounts mir mitteilte, dass ich einen neuen Follower hatte – CryptoRocky. Nun sind neue Twitter-Follower nichts Bemerkenswertes aber CryptoRockys Name weckte mein Interesse, also sah ich mir sein Profil an. Die Person, die hinter dem Twitterhandle »CryptoRocky« steht, heißt im realen Leben Roc Zacharias und ist angeblich Präsident einer Beratungsagentur, die sich auf »Zukunftstechnologien« spezialisiert. Welche »Zukunftstechnologien« das

sind, erfährt man bereits aus Zacharias' Profiltext bei Twitter: »President of Lunar Digital Assets. Crypto Enthusiast and Educator. Elon Musk, Tesla, SpaceX Fanboy. Bitcoin & Crypto will change EVERYTHING.«³

Zacharias' Selbstaussage kann hier stellvertretend stehen für die Firma, die er vertritt, aber auch für eine ganze Gruppe von Enthusiasten, mal direkt im Silicon Valley beheimatet, mal global verstreut, die so etwas wie einer kalifornischen Ideologie der Machbarkeit durch permanente Disruption, Innovation und *serial entrepreneurship* anhängen. Man könnte sie ›Technohurratrioten‹ nennen, deren persönliches Idol eben Figuren wie Elon Musk oder Ray Kurzweil sind. Was Zacharias zu einem guten Vertreter dieser Gruppe macht, ist nicht nur das Wortgeklingel der Digitalisierten, sondern der radikale Impetus, mit dem er propagiert, dass einige wenige Technologien alles radikal ändern können: »Bitcoin & Crypto will change EVERYTHING«.

Natürlich haben wir als Gesellschaft alle lernen müssen, dass viel von dem vor-dergründig absurden Gerede der Disruptoren dann doch die ökonomische Welt umkrempeln kann. Groß war jeweils das Gelächter bei Börsengängen wie dem von Facebook, weil sich die prädigitale Welt nicht ausmalen konnte, welche Wertschöpfung hinter einem reinen Datenunternehmen wie Facebook stehen könnte. Diese gepflegte prädigitale Unwissenheit existiert selbst nach dem bahnbrechenden »planetarischen« – um mit Heidegger zu sprechen – Erfolg von Facebook,



wenn etwa der damals 84-jährige Senator Orin Hatch Mark Zuckerberg bei der berühmt gewordenen *Senatsanhörung* am 10. April 2018 fragt: »So, how do you sustain a business model in which users don't pay for your service?« Der prädigitalen Unwissenheit von Hatch steht Roc Zacharias exemplarisch entgegen als der hyperdigitale Glaube, dass sich eine Disruption nahtlos an die andere reiht. Der heilige Gral und das Geschäftsmodell von Zacharias ist dabei »Bitcoin & Crypto«, stellvertretend für sogenannte Kryptowährungen und die diesen zugrunde liegende Technologie der *Blockchain*.

³ Twitterprofil von Roc Zacharias: <https://twitter.com/CryptoRocky> (02.01.2019). Zacharias war übrigens ein kurzlebiger Twitterfollower, der mir nach etwa einer Woche wieder entfolgte.

Der *Blockchain/Bitcoin*-Hype scheint inzwischen abgeflaut. Das berühmte *Bitcoin*-Hoch, als der Preis für einen Bitcoin am 17. Dezember 2017 auf die nie wieder erreichte Marke von 19.783 Dollar stieg, ist vorbei. Andererseits haben sich die wichtigsten Kryptowährungen wie *Bitcoin*, *Ethereum* und *Ripple* längst zu echten Investmentmöglichkeiten gemausert, die zwar hochvolatil sind, aber mittlerweile von diversen institutionellen Anlegern anerkannt sind. Selbst Groß- und Zentralbanken kaufen und handeln inzwischen Kryptowährungen.

Kryptowährungen sind damit so etwas wie das längst vertraute Gesicht der Technologie *Blockchain* geworden, die sich angeblich anschickt, eben alles zu verändern, indem es in jene dritte Welt der Drei-Welten-Ontologie eingreift. Hätte Zacharias Recht, dann würde unterhalb des Tones, den Supermarktangestellte auslösen, wenn sie Waren scannen, demnächst stets *Blockchain*-Technologien laufen.

3. *Blockchains* für Alle und jedes

Wie so oft bei Medientechnologien lohnt sich ein Blick unter die metaphorische Motorhaube, abseits vom Gerede der *Cryptowonks*. Und wie so oft lohnt es sich nicht, die Theoretiker dazu zu befragen, sondern die Techniker, die Schaltpläne, die Bedienungsanleitungen. Eine solche ist der kurze Text *Five Blockchain Ground Rules*, den der Informatiker und IT-Unternehmer Jaroslav Blaha am 8. Februar 2018 auf seiner LinkedIn-Seite veröffentlichte. Als kurze Anleitung für die Frage, ob die *Blockchain* eine passende Lösung für ein Problem darstellt, werden die Grundprinzipien der *Blockchain* auf ihre vielleicht kürzest mögliche Zusammenfassung reduziert. Wegen der instruktiven Kürze hier der Text in ganzer Länge:

»Jaroslav Blaha, CEO Cellmatiq, 8. Feb. 2018

Five Blockchain Ground Rules

Blockchain is the latest hype and everybody is building startups to do »something« with it. Most of those ideas are ridiculous. That is because very few people actually understand the math, the concepts, and the underlying limitations. Before you invest, consider at least the most important rules:

1. Blockchain is a de-centralized database designed with the explicit intent to avoid any centralized component. If you need or can tolerate central authority or components, then it is the wrong solution. A simple classical database does the job.
2. De-centralized databases have inherently heavy complexity and performance penalties. By their very math, they only provide »eventual transaction consistency« with no guarantee for transaction completion (i. e. if the transaction ever goes through then it will be OK). If you need transaction safety with time constraints, a simple classical database does the job.

3. The underlying byzantine consensus protocols require plenty of time to achieve a stable transaction state. That is why e. g. Bitcoin processes only ca. 7 transactions per second and Ethereum up to 20—globally and in competition to all other use cases. If you need fast and deterministic transaction behavior, a simple classical database does the job.
4. Brutally abbreviated, the truth of what is stored in each new block is defined by the block's miner and endorsed by 50+% of the nodes. In each, Bitcoin and Ethereum, just three mining pools already own this majority of new blocks. It would be fairly easy for those pools to join forces and to rig the system to their advantage. If such risk is not acceptable, a simple classical database does the job.
5. It would be feasible to bypass a subset of the above limits by adapting some of the open source code and to develop your bespoke blockchain implementation. But unless you convince a huge number of users to follow you by building and running nodes for your chain, you become the central component, which totally defies the purpose.

Clearly, there are very valid use cases for blockchain implementations and I am also convinced that this technology will open spectacular new opportunities. But, dear startups, please read a textbook on the facts first.

If you can live with all the above limitations (and there are many more) then go ahead with your blockchain initiative. Otherwise: A simple classical database really does the job!⁴

Damit ist die technische Seite *in nuce* gut erklärt. *Blockchain* ist eigentlich nichts anderes als eine dezentralisierte Datenbank mit allen ihren Vorteilen und Nachteilen. Das Hauptaugenmerk liegt auf der Vermeidung von möglichen Zentralautoritäten, Souveränen über die Blockchainprozesse. Es klingt nach Demokratie, Transparenz, Gleichheit, sichergestellt durch eine globale, weil möglichst total dezentralisierte Verteilung der Nodes, die die *Blockchain* prozessieren.

Gefühlt fast abseits dieser reinen Technizitäten existiert eben jener oft absurd anmutende und vielleicht komplett fehlgeleitete *Blockchain*-Hype, den es zum einen in einer inzwischen historischen Variante gibt, deren ehemalige Befürworter heute ihren damaligen Technohurratriotismus etwas kritischer sehen, wie etwa Manouhehr Shamsrizi, von dem ein Profiltext behauptet: »Er gilt als »innovativer Visionär« (TED), »Shootingstar der StartUp-Szene« (Hamburger Morgenpost) und ist laut Washington Post »among the most publicly prominent voices of Germany's younger generation.«⁵

⁴ Jaroslav Blava: Five Blockchain Ground Rules, unter: <https://www.linkedin.com/pulse/five-blockchain-ground-rules-jaroslav-bl%C3%A1ha/> (01.02.2019).

⁵ Profiltext Shamsrizis auf der Seite des interdisziplinären Labors *Bild Wissen und Gestaltung* im Hermann von Helmholtz-Zentrum für Kulturtechnik, unter <https://www.interdisciplinary-laboratory.hu-berlin.de/de/content/manouhehr-shamsrizi/> (02.02.2019).

Shamsrizi könnte also durchaus stellvertretend stehen für eine Szene zwischen wissenschaftlichem Lab, Entrepreneur-Clustern, Politikberatung und NGOs, die einstmals die *Blockchain* als Heilsbringer und Lösung für alles bezeichnet haben. Shamsrizi selbst blickt belustigt auf die eigene Begeisterung zurück, wenn er einen Tweet des Accounts Coinspondent vom 17. Juni 2015, der die Umstellung der gesamten Bundestags-IT-Architektur auf *Blockchain*-Technologie aufbauen wollte, kommentiert mit: »Was wir so 2015 für #blockchain-Träume geträumt haben.«⁶

Diesem neugewonnenen Realismus gegenüber steht eine anscheinend immer noch ungebrochene Begeisterung für den – auch gerne völlig sinnfreien – Einsatz von *Blockchains*. So findet sich auf der Webseite des Handelsblatts im März 2019 ein von Siemens gestalteter PR-Beitrag, der optisch wie ein redaktioneller Beitrag des Handelsblatts daherkommt und unter dem launigen Titel *Blockchain macht Kartoffelchips sicherer* das Siemens-eigene Blockchain-Produkt *Mindsphere* bewirbt, mit dem Supply-Chain-Management-Prozesse angeblich genauere Identifikation von Produktionschargen ermöglichen:

»Per Blockchain hätte etwa ein in Frankfurt ansässiger Kartoffelchips-Hersteller, der seine Kartoffeln aus Deutschland, das Salz aus Frankreich und das Sonnenblumenöl aus Italien bezieht, sofortigen Zugriff auf alle relevanten Informationen: Wo und wie wurden die Kartoffeln beim Bauern gelagert? Unter welchen Bedingungen verlief die Auslieferung? Wurde dabei auf alle Lebensmittelstandards geachtet? Sind die Kartoffeln korrekt geschält, gewaschen, geschnitten und getrocknet worden? Hatte das Öl die richtige Temperatur? Wurde die richtige Menge an Salz beigemischt? Verlief die Auslieferung in den Handel einwandfrei?«⁷

Das ist natürlich reichlich hanebüchen, geht es doch hier um einfache digitalisierte Aus- und Aufzeichnung von Produktchargen. Das angebliche Argument für die *Blockchain*-Nutzung ist dann auch keines, obwohl die Siemens-Werbung es so präsentiert: Basierend auf dem offenen, cloudbasierten IoT-System *MindSphere* sollen Zulieferer, Distributoren und Hersteller Daten bei jedem Schritt in der Transport- und Produktionskette sammeln und diese in einer *Blockchain* speichern. Diese Art der digitalen und fälschungssicheren Dokumentation ist besonders interessant für Hersteller, die ihre Lebensmittel weltweit vertreiben und deren Zutaten sie global beziehen. »Durch die Blockchain hätte man eine sehr starke Eingrenzung auf eine bestimmte Charge, einen bestimmten Produktionstag, den man

⁶ Tweet Shamsrizis von seinem Account @manouatwork am 02.05.2019, unter: <https://twitter.com/manouatwork/status/1124006158367449093> (02.05.2019).

⁷ Siemens-PR-Beitrag auf der Webseite des Handelsblatts vom 2. März 2019, unter: <https://www.handelsblatt.com/adv/siemens-digital/digitaler-leckerbissen-blockchain-macht-kartoffelchips-sicherer/24120902.html> (02.03.2019).

zurückrufen lassen könnte«, sagt Matthias Povolny, der bei Siemens im Account Development Team für die Analyse neuer Marktoptionen verantwortlich ist. Das Risiko, dass verseuchte Lebensmittel in den Handel kommen, könne man ihm zufolge so deutlich minimieren. Das gilt auch für grundlose Rückrufe.⁸ Selbst eine oberflächliche Lektüre der Zeilen macht klar, dass das, was Siemens hier als Lösung verkaufen will, mit anderen technischen Verfahren als der Blockchain effizienter zu lösen wäre. Um hier nochmal den Pragmatiker Blaha zu zitieren: »A simple classical database really does the job!« Aber worin lag – oder liegt noch immer – jenes mythische Versprechen der *Blockchain*, das Siemens nur als Letzter in einer Kette zu einem sinnlosen Marketing-Argument macht?

4. Das Versprechen der *Blockchain* oder die *Schmittcoin*

Am 1. April dieses Jahres schlug der Wiener Kurator und Medienwissenschaftler Paul Feigelfeld in einem lakonischen Tweet so etwas wie eine satirische Cryptowährung vor: *Schmittcoin*. *Schmittcoin* – benannt nach dem Theoretiker des Souveräns, dem Juristen Carl Schmitt – wäre, so Feigelfeld, »a sovereignty-based recentralized Carl Schmitt inspired token«.⁹ Damit dreht er passend zum Veröffentlichungsdatum des Tweets die Logik von *Blockchain*-basierten Währungen um und erklärt *ex negativo* den wichtigsten Punkt – das Versprechen der *Blockchain*-Anwendungen: die Dezentralisierung, die sich einzelnen Souveränen, wie Schmitt sie analysiert hat, entzieht.

Im berühmt gewordenen Inauguraldokument der *Blockchain*- und Kryptobewegung, Satoshi Nakamotos Manifest *Bitcoin: A Peer-To-Peer Electronic Cash System*, offenbart sich der Grund, das Verlangen, das vielleicht immer noch, subkutan, selbst die letzte und unsinnigste *Blockchain*-Anwendung legitimieren will, eine Erosion des Vertrauens:

»Commerce on the Internet has come to rely almost exclusively on financial institutions serving trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.«¹⁰

⁸ Ebd.

⁹ <https://twitter.com/paulfeigelfeld/status/1112697010799460352> (01.04.2019).

¹⁰ Satoshi Nakamoto: *Bitcoin: A peer-To-Peer Electronic Cash System*, unter: <https://bitcoin.org/bitcoin.pdf> (01.02.2019).

Es geht also um die »inherent weaknesses of the trust based model«. Vertrauen ist bei Zahlungen etwas, das ich in ökonomischen Dingen eben nicht nur beim Käufer und Verkäufer, sondern auch den zentralen Institutionen gegenüber aufbringen muss, die das System der Zahlung, die Währung, in der gezahlt wird, beherrschen und garantieren. Die Geldwirtschaft war in diesem Sinne übrigens schon lange vor der Existenz dieses Begriffes eine reichlich monopolistische *Platform Economy*. Darüber hinaus eskaliert die Krise des Vertrauens, weil elektronische monetäre Transaktionen aufgrund ihrer Elektronizität eben eine weitere Ebene der Repräsentation sind, die auch noch reversibel sind: »With the possibility of reversal, the need for trust spreads.«¹¹

Braucht es bei Barzahlungen bereits das Vertrauen, dass für das Bargeld eine entsprechende Menge Waren zu erhalten sind, hat sich mit der Virtualisierung des Geldes noch eine weitere Ebene der potenziellen Verunsicherung aufgetan. War Papiergeld einstmals die Garantie für eine bestimmte Menge von Edelmetall, so wurde es spätestens nach Auflösung diverser Gold- und Silberstandards nur noch ein Vertrauen in eine Zentralinstitution, die selbst zum Garanten nun diffuserer Werte wurde. Und vielleicht ist es eine selbstironische Volte, dass die US-Zentralbank dieses Vertrauen nochmals an übergeordnete Institutionen diffuserer Art delegiert, wenn sie auf Dollarschein *In God we trust* druckt. Digitale und digitalisierte Transaktionen eskalieren also ein bereits bestehendes soziales Problem von ausdifferenzierten Gesellschaften:

»Mit der Ausdifferenzierung einer Gesellschaft, die Sprache benutzt und Zeichen verwendet, entsteht das Problem des *Irrtums* und der *Täuschung*, des *unabsichtlichen* und des *absichtlichen Mißbrauchs der Zeichen*. Dabei geht es nicht nur um die Möglichkeit, daß die Kommunikation gelegentlich mißglückt, in die Irre geht oder auf einen Irrweg geführt wird. Vielmehr ist dieses Problem, da dies *jederzeit* passieren kann, *jederzeit* präsent – eine Art Universalproblem des von Hobbes am Falle der Gewalt entdeckten Typs. Mit Bezug auf dieses Problem kann man verstehen, daß die Gesellschaft Aufrichtigkeit, Wahrhaftigkeit und dergleichen moralisch prämiert und im Kommunikationsprozeß auf Vertrauen angewiesen ist. Aber damit ist nur bestätigt, daß nicht vorkommen sollte, was doch möglich bleibt. Fragt man nochmals nach, wie der Kommunikationsprozeß selbst auf dieses Problem reagiert, dann sieht man den Vorteil der Codierung, denn sie ermöglicht es, etwas Mitgeteiltes zu bezweifeln, es nicht anzunehmen, es explizit abzulehnen und diese Reaktion verständlich auszudrücken, sie also in den Kommunikationsprozeß selbst wiedereinzubringen. Die Bezugnahme auf psychische und moralische Qualitäten wie Aufrichtigkeit und Vertrauen behält ihren Sinn, aber da kein Kommunikationsprozeß psychische Prämissen dieser Art prüfen kann (die Prüfung selbst würde das, was sie

¹¹ Ebd.

sucht, zerstören), müssen die Bedingungen psychologisch dekontingiert werden und als Themen der Kommunikation selbst behandelt werden.«¹²

Luhmanns soziologische Diagnose ist somit die perfekte Beschreibung für die Garantie- und Vertrauensbedürfnisse eines Kommunikationssystems, das auf dem Prinzip der Lacan'schen ›Anleimung‹ basiert. Innerhalb des Systems muss darauf vertraut werden, dass die Anleimungen korrekt sind. Das verdient unter heutigen Bedingungen ein Update, wenn die neuen Technizitäten – etwa von elektronischen Transaktionen – mitbedacht werden sollten, was *de facto* auf nahezu alle unsere heutigen Transaktionen zutrifft, unter anderem an der Supermarktkasse. In diesen Fällen wird das Vertrauensproblem auf der Ebene der Digitalität jedoch nicht wiedereingeführt (als Selbstverständigung des soziologischen Systems à la Luhmann), sondern ganz handfest nochmals *ausgeführt*, iteriert, prozessiert, implementiert. Die *Blockchain* könnte daher als technischer Versuch gewertet werden, innerhalb des nun auch technisch gewordenen Kommunikationssystems eine technische Antwort auf eine soziologische Frage zu finden, die sich eskalatorisch neu und härter gestellt hat.

Nakamotos Idee von *Bitcoin* ist dementsprechend die Etablierung eines »electronic payment system based on cryptographic proof instead of trust«¹³ – also die Ersetzung der soziologisch-systemischen Resource Vertrauen durch eine technische Operation.

Was hierbei nicht bedacht wird, ist, dass dabei lediglich wieder eine Verschiebung des Vertrauens stattfindet. Die angebliche Ersetzung von Vertrauen durch technische Prozesse ist lediglich eine Metonymie. Denn auch den technischen Prozessen muss vertraut werden. Und vielleicht ist es die vermeintliche oder tatsächliche Undurchsichtigkeit von algorithmischen Prozessen, die solche Verschiebungen erst möglich macht: von in »Go(l)d we trust« zu »In algos we trust«. Das kann man dann auf angeblich alle digitalen Prozesse anwenden, egal ob sie Geld oder Kartoffelchips steuern.

Nakamoto selbst verbirgt das Problem seiner und aller *Blockchain*-Prozesse im Hinblick auf die mögliche Ersetzung von Vertrauen durch algorithmische Prozesse rhetorisch in einem kurzen und banal klingenden Satz, dessen enorme Tragweite nicht weiter ausgeführt wird:

»The System is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.«¹⁴ Für die reale Implementierung der wichtigs-

¹² Niklas Luhmann: Die Gesellschaft der Gesellschaft, Frankfurt am Main 1998, S. 225 f.

¹³ Nakamoto: Bitcoin (wie Anm. 10).

¹⁴ Ebd.

ten Kryptowährungen zeigt sich dann bei genauerem technischen Hinsehen die Nicht-einlösbarkeit dieser Hoffnung: »In each, Bitcoin and Ethereum, just three mining pools already own this majority of new blocks. It would be fairly easy for those pools to join forces and to rig the system to their advantage.«¹⁵



Am Ende entbergen sich die Versprechungen der Dezentralität als technisch nicht einlösbar. Algorithmen laufen eben doch auf echten Computern, durch Nodes, die kontrollierbar sind. Das berühmte kritische Memebild darüber, dass die ›Cloud‹ am Ende doch nur der Computer eines anderen ist, gilt auch für *Blockchain*-Anwendungen. Wer Nodes kontrolliert, kontrolliert die

Blockchain. Am Ende also doch wieder (Techno-)Territorialität, Territorien und Prozesse, über die Souveräne entscheiden. Deswegen ist der *Bitcoin* vielleicht doch ein *Schmittcoin* – aber das wäre weit ab von den Heilsversprechen, mit denen man Lösungen für Kartoffelchips oder Demokratieprojekte bewerben kann.

¹⁵ Blaha: Five Blockchain Ground Rules (wie Anm. 4).

Hype oder Horror

Potenziale und Hürden der Blockchain-Technologie anhand rechtlicher Rahmenbedingungen

Cathrin Hein / Wanja Wellbrock / Christoph Hein

1. Einleitung

Die *Blockchain*-Technologie wird oftmals als »biggest opportunity set we can think of over the next decade« beschrieben.¹ Andere sehen das Potenzial darin: »What the internet did for communications, blockchain will do for trusted transactions.«² Wieder andere übertreiben etwas, wenn sie *Blockchain* als »eine Technologie die unser ganzes Denken revolutioniert« feiern.³ Aber was hat es mit dieser angeblich revolutionären Technologie auf sich?

Blockchain ist eine Basistechnologie, auf deren Grundlage neue Plattformen und Geschäftsmodelle geschaffen werden können.⁴ Der bekannteste Anwendungsfall der *Blockchain*-Technologie dürfte die Kryptowährung *Bitcoin* sein. Im Jahre 2008 veröffentlichte eine unbekannte Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto das *Bitcoin* Whitepaper *Bitcoin: A Peer-to-Peer electronic Cash System*⁵ als Blaupause für digitale Währung.⁶ Dies wird oft als die Reaktion der digitalen Gemeinschaft auf die weltweite Finanzkrise gesehen, in deren Folge vor allem Banken massiv an Vertrauen eingebüßt hatten. Digitale Währungen auf Basis der *Blockchain*-Technologie kommen ohne entsprechende Intermediäre bei den Transaktionen aus.⁷

¹ Sweta Jaiswal: Is Blockchain a Game-Changer for Healthcare?, unter: <https://www.nasdaq.com/article/is-blockchain-a-game-changer-for-healthcare-cm944721> (06.04.2018).

² Graham Rapiere: From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world, unter: <https://www.businessinsider.de/ibm-ceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6?r=US&IR=T> (21.07.2017).

³ Milosz Matuschek: Blockchain – eine Technologie revolutioniert unser ganzes Denken, unter: <https://www.nzz.ch/meinung/kommentare/new-kids-on-the-blockchain-ld.1319020> (02.10.2017).

⁴ Stephan Breidenbach und Florian Glatz: *Rechtshandbuch Legal Tech*, München 2018.

⁵ Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*, unter: <https://bitcoin.org/bitcoin.pdf> (10.06.2008).

⁶ Breidenbach und Glatz: *Rechtshandbuch Legal Tech*, (wie Anm. 4).

⁷ Christian Siedenbiedel: *Bitcoins: Aufstieg und Fall einer seltsamen Währung*, unter:

Per Definition ist *Blockchain* eine dezentrale Datenbank, die aus einer stetig größer werdenden Liste von Datensätzen besteht, welche verteilt auf unterschiedlichen Computern gesichert werden. Dabei werden die Transaktionen in Blöcken zusammengefasst und die Prüfsumme des Vorgängerblocks stets als Validierungsmerkmal mitgegeben. Diese Technik wird auch als *Distributed Ledger*-Technologie bezeichnet.⁸

Es stellt sich hierbei die Frage, ob das deutsche Rechtssystem grundsätzlich in der Lage ist, die Herausforderungen, die diese dezentrale Technologie mit sich bringt, zu bewältigen. Bisher gibt es hierzulande noch keine konkreten rechtlichen Regelungen in puncto *Blockchain*. Andere Länder sind hier weiter. In Thailand trat am 13. Mai 2018 ein Gesetz für den Umgang mit Kryptowährungen in Kraft.⁹ Der US Bundesstaat Michigan hat einen Gesetzesentwurf vorgestellt, nachdem es strafbar ist, Datensätze, die unter der Verwendung von *Distributed Ledger*-Technologie gespeichert werden, zu ändern.¹⁰ Der US Bundesstaat Tennessee definiert *Blockchain*-Technologie gesetzlich wie folgt: »Blockchain technology means distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth.«¹¹

Eine Studie der Rheinisch-Westfälischen Technischen Hochschule Aachen und der Goethe-Universität Frankfurt wirft darüber hinaus die Frage auf, ob Nutzer eines *Blockchain*-Netzwerkes für rechtswidrige Inhalte verantwortlich gemacht werden können. Im Rahmen der Studie wurden die nichtfinanziellen Inhalte der *Bitcoin-Blockchain* analysiert und dabei u. a. Links zu Kinderpornographie entdeckt. Jeder Nutzer der *Bitcoin-Blockchain* hat per Definition eine Kopie sämtlicher Datensätze auf dem genutzten Computer und könnte sich dadurch strafbar machen.¹²

<http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/bitcoin-aufstieg-und-fall-einer-seltsamen-waehrung-12848847.html> (05.03.2014).

⁸ Alexander Djazayeri: Rechtliche Herausforderungen durch Smart Contracts, in: jurisPR-BKR 12/2016 Anm. 1 (20.12.2016).

⁹ Roman Maas: Thailands neues Krypto-Gesetz tritt in Kraft, unter: <https://www.btc-echo.de/thailands-neues-krypto-gesetz-tritt-in-kraft/> (16.05.2018).

¹⁰ Tanja Giese: Michigan – Unveränderlichkeit der Blockchain soll Gesetz werden, unter: <https://www.btc-echo.de/michigan-unveraenderlichkeit-der-blockchain-soll-gesetz-werden/> (16.06.2018).

¹¹ Tennessee Generalversammlung: House Bill 1507, Tennessee (USA), unter: <http://www.capitol.tn.gov/Bills/110/Bill/HB1507.pdf> (26.03.2018).

¹² Hendrik Wieduwilt: Problem für Zukunftstechnologie – Kinderpornographie in der Blockchain gefunden, unter: <http://www.faz.net/aktuell/wirtschaft/diginomics/kinder-pornographie-in-blockchain-gefunden-15507813.html> (23.03.2018).

Es ist unstrittig zu erkennen, dass insbesondere rechtliche Aspekte in der Zukunft eine große Rolle im Umfeld *Blockchain*-basierter Applikationen spielen werden. Für eine Auseinandersetzung mit den rechtlichen Herausforderungen für Privatpersonen und Unternehmen ist es daher unvermeidbar, dass Sie sich ein grundlegendes Verständnis der zugrunde liegenden Technologie aneignen und sich den rechtlichen Risiken und Unschärfen einer Nutzung bewusst sind.

2. Blockchain-Technologie

Bitcoin gilt als der Ursprung der *Blockchain*-Technologie. Hiervon leiten sich die technologischen Eckpfeiler des Systems ab. Es handelt sich um ein dezentrales Netzwerk, innerhalb dessen eine künstlich begrenzte Menge an Wertmarken generiert wird. Während diese Wertmarken eindeutig einem Benutzer zugeordnet werden können, bleibt selbiger anonym. Analog den Banken in der realen Welt wurde vor *Bitcoin* stets eine zentrale Instanz benötigt, um die Transaktionen zu kontrollieren und das *Double Spending* zu verhindern. Eine Einheit einer Kryptowährung darf ebenso nur einmal verwendet werden, wie in früheren Zeiten ein Scheck.¹³

Innerhalb einer *Blockchain* werden sämtliche Transaktionsdaten gespeichert und neue Transaktionen fortlaufend mit der bestehenden Transaktionshistorie abgeglichen und so geprüft, ob ein Wert bereits vorher ausgegeben wurde.¹⁴

Die Basis *blockchain*-basierter Anwendungen ist der dezentrale Aufbau des Netzwerks. Während es bei einem zentralisierten Netzwerk eine entsprechende Instanz gibt, die die getätigten Transaktionen verwaltet und kontrolliert, verzichtet ein dezentrales Netzwerk auf eben jene Kontrollinstanz und ermöglicht eine direkte Kommunikation zwischen den Teilnehmern, bei der jeder Teilnehmer jederzeit über den einheitlichen Datenbestand verfügt. Derartige Netzwerke sind von außen nicht zu kontrollieren (siehe Abb. 1, S. 134).

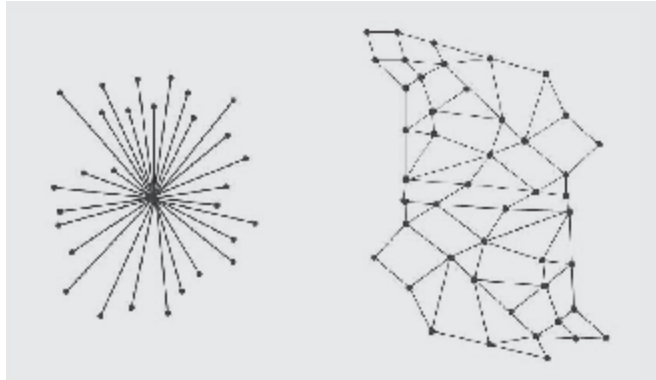
Blockchain-Netzwerke sind nicht nur auf die Übertragung von Kryptowährungen ausgelegt. Es können beispielsweise auch im Rahmen von *Smart Contracts* Kaufverträge darüber dokumentiert werden, da alle Transaktionen öffentlich nachvollziehbar sind. Man spricht hier auch vom Internet der Werte (*Internet of Value*), in dem jede Übertragung von Gütern abgebildet werden kann.¹⁵

¹³ Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

¹⁴ Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431–1436.

¹⁵ Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: Blockchain – Hype oder Innovation, Technischer Bericht Nr. 113, unter: <https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf> (20.09.2018).

Abb. 1:
Zentraler vs. dezentraler Netzwerkaufbau (Stephan Breidenbach und Florian Glatz: Rechtshandbuch Legal Tech, München 2018)



Hierfür werden initial die Vermögenswerte innerhalb des Netzwerks definiert, aufgelistet und den Eigentümern zugeordnet. Für diese Assets erhalten die jeweiligen Eigentümer sogenannte *Tokens*. Diese repräsentieren im weiteren Verlauf das Eigentum am jeweiligen Vermögenswert wodurch so erstmals effektiv das *Double Spending* verhindert werden kann.¹⁶

Mangels zentraler Instanz verfügen alle Teilnehmer einer *Blockchain* über die gleiche Legitimation innerhalb des Netzwerks. Jeder Teilnehmer hat theoretisch die gesamte Transaktionshistorie gespeichert. Da diese bei *Bitcoin* beispielsweise bereits 147 GB beträgt (Stand Dezember 2017), unterscheidet man inzwischen in sogenannte *Lightweight Nodes* und *Full Nodes*. Erstere speichern lediglich den für sie relevanten Teil der *Blockchain*, letztere dagegen den gesamten Datenbestand.

Ausgangspunkt für die Teilnahme am *Bitcoin*-Netzwerk ist die sogenannte *Wallet*. Diese stellt allerdings keine Geldbörse im eigentlichen Sinne dar, sondern dient lediglich der Verwaltung des *Blockchain*-Kontos. Die Adresse selbiger ist pseudonymisiert und dient der Kontoverwaltung und dem Senden und Empfangen von Transaktionen.¹⁷ Die Transaktionen werden mittels *Public Key*-Verfahren verschlüsselt, wodurch sichergestellt wird, dass nur berechtigte Teilnehmer Transaktionen vornehmen.¹⁸

¹⁶ Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

¹⁷ Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15).

¹⁸ Daniel Burgwinkel: Blockchain Technology – Einführung für Business- und IT Manager, Berlin und Boston 2016; Joachim Schrey und Thomas Thalhofer: Rechtliche Aspekte der Blockchain, in: NJW – Neue Juristische Wochenschrift 70/20 (2017), S. 1431–1436; Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, unter: <https://bitcoin.org/bitcoin.pdf> (10.06.2008).

Am Beispiel der *Bitcoin-Blockchain* enthalten die Transaktionen primär Informationen über die Herkunft und den Empfänger der *Bitcoins*. Die Besonderheit hierbei ist, dass keine *Bitcoins* in der Quelle übrigbleiben dürfen. Hat man zwanzig *Bitcoins* und möchte nur fünf davon an einen anderen Nutzer überweisen, ist es notwendig, sich die restlichen fünfzehn *Bitcoins* selbst zu überweisen. Ansonsten würde die Differenz als Transaktionsgebühr für den Nutzer verloren gehen. Der vollständige Datensatz wird an die übrigen Teilnehmer des Netzwerks gesendet und zunächst zwischengespeichert, bis er final in einen Block aufgenommen wird.¹⁹

Alle Transaktionen innerhalb der *Blockchain* werden in Blöcken gespeichert. Sie umfassen bei der *Bitcoin-Blockchain* beispielsweise ungefähr 900 bis 2.500 Transaktionen pro Block. Vor der Aufnahme in einen Block werden die Transaktionen validiert, um zu verhindern, dass bereits ausgegebene *Bitcoins* nicht erneut ausgegeben werden. So entsteht die unveränderbare Transaktionskette, das Markenzeichen der *Blockchain*.²⁰

Die sogenannten *Miner* – Computer, die dem Netzwerk Rechenleistung bereitstellen – schließen die Blöcke, errechnen die mathematisch generierte Identifikationszahl und verknüpfen den Block mit dem vorherigen Block in der Kette (siehe Abb. 2, S. 136). Die Ermittlung dieses einmaligen Fingerabdrucks benötigt eine hohe Rechenleistung aufgrund der hohen Anzahl führender Nullen, sogenannter *Nonce*. Dieser Prozess stellt die Datenintegrität in der *Blockchain* sicher und ermöglicht, dass die Transaktionen nachträglich nicht mehr verändert werden können.²¹

¹⁹ Gayvoronskaya, Meinel und Schnjakin: *Blockchain – Hype oder Innovation*, (wie Anm. 15); Stefan Groß und Axel-Michael Wagner: *White Paper. Blockchain und Smart Contracts – Moderne IT-Konzepte aus (datenschutz-)rechtlicher Sicht*, unter: https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf (10.03.2018).

²⁰ Gayvoronskaya, Meinel und Schnjakin: *Blockchain – Hype oder Innovation*, (wie Anm. 15); Joachim Schrey und Thomas Thalhofer: *Rechtliche Aspekte der Blockchain*, in: *NJW – Neue Juristische Wochenschrift* 70/20 (2017), S. 1431–1436; Stephan Breidenbach und Florian Glatz: *Rechtshandbuch Legal Tech*, München 2018.

²¹ Breidenbach und Gatz: *Rechtshandbuch Legal Tech*, (wie Anm. 4); Stefan Groß und Axel-Michael Wagner: *White Paper. Blockchain und Smart Contracts – Moderne IT-Konzepte aus (datenschutz-)rechtlicher Sicht*, unter: https://www.psp.eu/media/allgemein/white_paper_blockchain.pdf (10.03.2018); Joachim Schrey und Thomas Thalhofer: *Rechtliche Aspekte der Blockchain*, in: *NJW – Neue Juristische Wochenschrift* 70/20 (2017), S. 1431–1436; Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: *Blockchain – Hype oder Innovation*, *Technischer Bericht Nr. 113*, unter: <https://publshup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf> (20.09.2018); Daniel Drescher: *Blockchain Grundlagen – Eine Einführung in die elementaren Konzepte in 25 Schritten*, Frechen 2017; Daniel Burgwinkel: *Blockchain Technology – Einführung für Business- und IT Manager*, Berlin und Boston 2016.

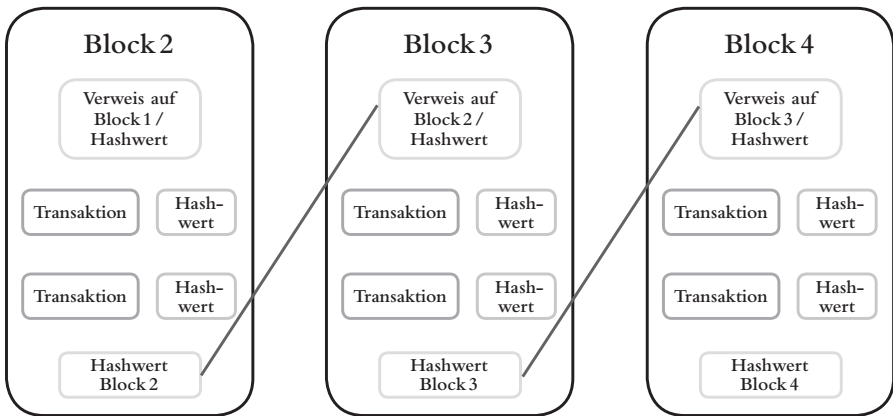


Abb. 2: Prinzip der *Blockchain*-Technologie (Daniel Burgwinkel: *Blockchain Technology – Einführung für Business- und IT Manager*, Berlin und Boston 2016)

Die Netzwerkteilnehmer sind oft weltweit verteilt, was Unterschiede in der Übertragungsgeschwindigkeit der Daten mit sich bringt. Dadurch kann es zu Ungleichgewichten im Datenbestand kommen, und es ist nicht immer gewährleistet, dass alle Daten zeitgleich bei allen Teilnehmern aktualisiert werden. Um dem entgegenzuwirken, sollte immer nur die längste Kette an Blöcken als valide akzeptiert werden.²²

Die Bereitstellung der Rechenleistung durch die *Miner* kostet Zeit und Geld und wird innerhalb der *Bitcoin-Blockchain* beispielsweise auf zwei Arten entlohnt. Einerseits wird für die Aufnahme in einen Block eine Transaktionsgebühr von den *Minern* erhoben und andererseits entstehen in jedem neuen Block neue *Bitcoins*, die der jeweilige *Miner* als Entschädigung erhält.²³

Blockchain ist nicht gleich *Blockchain*. Es gibt unterschiedliche Lösungsansätze auf Basis dieser Technologie. Eine Variante sind private Netzwerke, bei denen ein Beitritt zum geschlossenen Teilnehmerkreis nicht ohne weiteres möglich ist. Beispielhaft sei hier *Hyperledger* genannt, eine Initiative, die *Blockchain*-Anwendungen für Unternehmen entwickelt.²⁴

Im Gegensatz dazu ist bei den öffentlichen *Blockchain*-Anwendungen eine Teil-

²² Hans Bechtolf und Niklas Vogt: Datenschutz in der Blockchain – Eine Frage der Technik, in: ZD – Zeitschrift für Datenschutz 8/2 (2018), S. 66–70.

²³ Gayvoronskaya, Meinel und Schnjakin: Blockchain – Hype oder Innovation, (wie Anm. 15).

²⁴ Fraunhofer-Gesellschaft: Blockchain und Smart Contracts – Technologien, Forschungsfragen und Anwendungen, unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-

nahme für jedermann möglich und bedarf keiner gesonderten Erlaubnis, beispielsweise das schon erwähnte *Bitcoin* oder *Etherum*. Letzteres dient im Übrigen nicht einzig dem Austausch von Kryptowährung, sondern ist gleichzeitig auch eine *Smart Contracts*-Plattform.²⁵

Blockchain-Anwendungen setzen eine schnelle Internetverbindung und hohe Rechenleistung voraus. Letztere verursacht insbesondere durch den Stromverbrauch immense Kosten, was auch einer der größten Kritikpunkte an der *Blockchain*-Technologie ist. Gleichzeitig ist es auch der größte Schutz vor Manipulationen. Theoretisch müsste man nur 51% der Rechenkapazität innerhalb einer *Blockchain* kontrollieren und könnte anschließend die Anwendung nach Belieben manipulieren. Allerdings ist es eben aufgrund der hohen Kosten für die Bereitstellung der Rechenkapazität in der Regel lukrativer, diese einfach als *Miner* einzusetzen und dafür *Bitcoins* zu erhalten.²⁶

Trotz des geringen Restrisikos des Hackings gewährleistet die *Blockchain*-Technologie einen hohen Sicherheitsstandard, da die Daten dezentral verteilt, für alle Nutzer zugänglich und verschlüsselt sind. Der Verzicht auf Intermediäre, wie beispielsweise Banken, erlaubt eine schnellere Abwicklung und ermöglicht insbesondere in Regionen mit einem weniger stark ausgeprägten Rechtssystem, dass Verträge oder Überweisungen korrekt und sicher ausgeführt werden.²⁷

Die zugrunde liegende Technologie ermöglicht eine sichere Transaktionsabwicklung und ein gegenseitiges Vertrauen der Vertragspartner ist nicht notwendig. Es wird die gesamte Transaktionshistorie nachvollziehbar abgebildet und Nutzer können diese jederzeit einsehen. Außerdem arbeiten *Blockchain*-Netzwerke autonom, weshalb sich äußere Einflüsse nicht auf das Netzwerk auswirken²⁸

Contracts.pdf?_=1516641660 (10.11.2017); Linux Foundation: Hyperledger Business Blockchain Technologies, unter: <https://www.hyperledger.org/projects> (20.10.2018).

²⁵ Burgwinkel: Blockchain Technology, (wie Anm. 18).

²⁶ Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4); Dennis Streichert: Vorteile und Nachteile der Blockchain-Technologie, unter: <https://www.blockchain-infos.de/vorteile-nachteile-blockchain/> (19.10.2018); Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, unter: <https://bitcoin.org/bitcoin.pdf> (10.06.2008).

²⁷ Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4); Dennis Streichert: Vorteile und Nachteile der Blockchain-Technologie, unter: <https://www.blockchain-infos.de/vorteile-nachteile-blockchain/> (19.10.2018).

²⁸ Burgwinkel: Blockchain Technology, (wie Anm. 18).

3. Kinderpornographie als Beispiel rechtlichen Handlungsbedarfs

Eingangs wurde bereits auf die gefundenen Links zu kinderpornographischem Material innerhalb des *Bitcoin*-Netzwerks hingewiesen.²⁹ Dies erfolgt vorwiegend über spezielle Transaktionstypen oder Notizfelder von Standard-Transaktionen.³⁰ Da innerhalb einer *Blockchain* fortlaufend alle Transaktionsdaten unveränderlich gespeichert und jedem Nutzer zugänglich sind, stellt sich zunächst die Frage, ob das bloße Speichern der Transaktionshistorie, welches Zugangsvoraussetzung für die Teilnahme am Netzwerk ist, mit dem strafbaren *Besitz von Kinderpornographie* nach § 184b Abs. 3 StGB gleichzusetzen ist. Allerdings reicht die Bereitstellung der Daten zum Abruf auf einem Server in der Regel nicht als Straftatbestand aus.³¹ Jedoch werden derzeit Änderungen des StGB im Deutschen Bundestag diskutiert, nachdem bereits der Abruf mittels Rundfunk oder Telemedien strafbar wäre.³² Hier sind also künftig noch Änderungen zu erwarten.

Anders stellt sich der Sachverhalt bei dem Tatbestandsmerkmal des Vorsatzes gem. § 15 StGB dar, werden hier doch Wissen und Wollen der Tatbestandsverwirklichung vorausgesetzt. Ein vorsätzliches Handeln zu unterstellen, wenn der originäre Zweck der Handel mit der Kryptowährung *Bitcoin* ist, scheint fraglich. Gerade weil es die bloße Nutzung des Netzwerks zu einer Straftat erklären würde, da sich irgendwo innerhalb des Netzwerks rechtswidrige Inhalte befinden könnten. Sollte sich eine derartige Lesart allerdings durchsetzen, gäbe es für die Technologie kaum noch praktische Anwendungsfälle.

Es stellt sich noch die Frage, ob die *Miner* aus strafrechtlicher Sicht eine andere Rolle in diesem Prozess einnehmen. Mittäter i. S. v. § 25 Abs. 2 StGB wären sie, wenn sie sich der Verbreitung mitschuldig machen und die Daten einem größeren, nicht mehr kontrollierbaren Personenkreis zugänglich machen.³³ Zwar stellen sie ihre Rechenleistung dem Netzwerk zur Verfügung und tragen durch das Schließen der Blöcke maßgeblich zur Verbreitung der Daten bei, andererseits prüfen sie

²⁹ Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohfeld und Klaus Wehrle: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin unter: https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf (10.03.2018).

³⁰ Blockchain Bundesverband e.V.: Blockchain – Chancen und Herausforderungen einer neuen digitalen Infrastruktur für Deutschland, Version 1.1, unter: https://bundesblock.de/wp-content/uploads/2017/10/bundesblock_positionspapier_v1.1.pdf (16.10.2017).

³¹ Eric Hilgendorf und Brian Valerius: Computer- und Internetstrafrecht – Ein Grundriss, 2. Auflage, Berlin und Heidelberg 2012.

³² Deutscher Bundestag: Gesetzeswurf der Fraktionen der CDU/CSU und SPD zur Änderung des Strafgesetzbuches vom 23.09.2014, Drucksache 18/2601, unter: <http://dipbt.bundestag.de/doc/btd/18/026/1802601.pdf> (23.09.2014).

³³ Urs Kindhäuser: Strafgesetzbuch Lehr- und Praxiskommentar, 7. Aufl., Baden-Baden 2017.

die Transaktionen nicht inhaltlich und haben somit keine Verantwortung für die Transaktionen der Nutzer und können keinen Einfluss auf selbige nehmen. Eine zentrale Kontrolle des Inhalts würde den eigentlichen Zweck des Netzwerks, beispielsweise den dezentralen Austausch von Kryptowährung, aushebeln. *Vorsatz* nach § 15 StGB kann ebenso wenig unterstellt werden. Zweck des Netzwerks ist der Handel mit Kryptowährung und die Motivation zur Teilnahme für die Miner ist finanzieller Natur.

Rechtswidrige Inhalte innerhalb von *Blockchain*-Transaktionen stellen einen neuen Sachverhalt dar, der rechtlich noch nicht ausreichend analysiert ist. Der Gesetzgeber sollte hier Rahmenbedingungen schaffen, um für den durchschnittlichen Nutzer Rechtsicherheit zu schaffen.

4. Datenschutzrechtliche Aspekte der Blockchain-Technologie

Die seit Mai 2018 für die EU-Mitgliedstaaten geltende Datenschutz-Grundverordnung muss auch in Deutschland für die Verarbeitung personenbezogener Daten angewendet werden. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen« und eine Identifizierung, ohne dass anderweitige Informationsquellen genutzt werden, ermöglichen. Allerdings ist vorab zu klären, ob in einer öffentlichen *Blockchain* überhaupt derartige Daten enthalten sind oder ob es sich vielmehr um anonymisierte Informationen handelt, bei denen betroffene Personen nicht mehr identifiziert werden können.³⁴

Innerhalb eines *Blockchain*-Netzwerks werden Pseudonyme anstelle von Klarnamen verwendet, wodurch eine unmittelbare Identifizierung der jeweiligen natürlichen Personen nicht möglich ist. Allerdings würde es sich immer noch um eine identifizierbare Person nach Art. 4 Nr. 1 DS-GVO handeln, wenn durch die Verknüpfung des Pseudonyms mit weiteren Daten ein Rückschluss auf die natürliche Person möglich wäre.³⁵ Es ist demnach fraglich, ob die Adresse eines Nutzers in einer *Blockchain* als Pseudonym gilt und die DS-GVO anwendbar wäre oder es sich aufgrund der Verschlüsselungsmechanismen bereits um anonyme Daten handelt und demnach das Datenschutzrecht keine Anwendung findet.³⁶ Die Adresse

³⁴ Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

³⁵ Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14); Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

³⁶ Benedikt Buchner und Jürgen Kühling: Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

eines Benutzers im *Bitcoin*-Netzwerk wird mittels einer Hash-Funktion generiert und ist prinzipiell als Pseudonymisierung anzusehen, da die Herstellung eines Personenbezugs für die Zukunft nicht ausgeschlossen werden kann.

Der relativen Theorie folgend ist die Identifizierung natürlicher Personen durch Dritte sehr weit gefasst und eine Anonymisierung nahezu ausgeschlossen. Allerdings lässt sich ein *Verantwortlicher* i.S.d. DS-GVO innerhalb eines *Blockchain*-Netzwerks nicht eindeutig identifizieren. So gesehen müsste die absolute Theorie Anwendung finden und demzufolge die Möglichkeiten, die eine dritte Partei zur Identifizierung ergreifen könnte, in Betracht gezogen werden. Fraglich ist demnach, welche Mittel eine andere Person nach allgemeinem Ermessen wahrscheinlich einsetzt, um die Person hinter dem Pseudonym zu identifizieren. Dabei müssen der technologische Fortschritt und die Verhältnismäßigkeit zwischen notwendigem Aufwand und Identifizierungsinteresse berücksichtigt werden.³⁷ Würden in der *Blockchain* beispielsweise Gesundheitsdaten verschlüsselt gespeichert werden, könnte ein höheres Identifizierungsinteresse unterstellt werden als etwa bei weniger sensiblen Daten.³⁸

Über die Verknüpfung von *Bitcoin*-Transaktionen mit der IP-Adresse des Nutzers können Rückschlüsse auf die Vermögensverhältnisse und das Verhalten des Nutzers erfolgen und dadurch eine Deanonymisierung der dahinterstehenden Person herbeigeführt werden.³⁹ Weiterhin kann die Identität durch die Verknüpfung mit Zusatzinformationen ermittelt werden, wie beispielsweise der Einkauf in einem Online-Shop und die daraus resultierende Lieferadresse.⁴⁰ Eine *Blockchain* hat immer auch ein vollständiges Profil aller Nutzer und ihrer Transaktionen. Am Beispiel der *Bitcoin-Blockchain* werden demnach sämtliche finanziellen Vorgänge lückenlos archiviert. Veröffentlicht eine Person ihre *Bitcoin*-Adresse, so ist es möglich, sämtliche Zahlungsvorgänge dieser Person nachzuvollziehen. Beispielsweise

³⁷ Johanna Hofmann und Paul Johannes: DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs – Begriffsklärung der entscheidenden Frage des sachlichen Anwendungsbereichs, in: ZD – Zeitschrift für Datenschutz 7/5 (2017), S. 221–225.

³⁸ Benjamin Talin: Blockchain – Möglichkeiten und Anwendungen der Technologie, unter: <https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/> (04.07.2018).

³⁹ Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251–1270; Alex Biryukov, Dmitry Khovratovich und Ivan Pustogarov: Deanonymisation of clients in Bitcoin P2P network, unter: <https://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf> (10.05.2019); Tatiana Gayvoronskaya, Christoph Meinel und Maxim Schnjakin: Blockchain – Hype oder Innovation, Technischer Bericht Nr. 113, unter: <https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf> (20.09.2018).

⁴⁰ Bechtolf und Vogt: Datenschutz in der Blockchain, (wie Anm. 22).

hat Wikileaks die eigene *Bitcoin*-Adresse veröffentlicht, um Spenden zu generieren.⁴¹ Durch die Veröffentlichung der Adresse ist es möglich, alle Transaktionen dieser Adresse zu analysieren und Rückschlüsse auf die Vermögensverhältnisse von Wikileaks zu ziehen. Bei der Generierung von Spenden kann diese Nachvollziehbarkeit von Vorteil sein. Bei natürlichen Personen stellt dies jedoch eher ein Risiko dar, dem höchstens durch die bereits erwähnte Verwendung stetig neuer Schlüssel für Transaktionen entgegengewirkt werden kann. Andernfalls lässt sich eine solche Profilbildung nicht verhindern, und es können innerhalb des *Bitcoin*-Systems oder auch in anderen *Blockchain*-Netzwerken Rückschlüsse auf die Vermögensverhältnisse gezogen werden. Ob es sich also um die Verarbeitung personenbezogener Daten handelt, hängt insbesondere von den Interessen und technischen Möglichkeiten des Verantwortlichen oder einer anderen Person ab.⁴²

Verantwortlicher nach Art. 4 Nr. 7 DS-GVO ist »die natürliche oder juristische Person, [...] die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet«. Dadurch soll einer Stelle die Verantwortung, u. a. für die Einhaltung der Datenschutzbestimmungen, zugewiesen werden. Allerdings zeichnet sich ein *Blockchain*-Netzwerk insbesondere durch die dezentrale Struktur und das Fehlen einer zentralen Verantwortlichkeit aus.⁴³

In der Praxis würde eine Kontrolle durch die *Miner* das Vertrauen in das Netzwerk und dessen Sicherheit erheblich beeinträchtigen. Daher achten *Miner* innerhalb des *Bitcoin*-Systems stets von sich aus darauf, dass sie den Grenzwert von 51 % nicht überschreiten. Eine gemeinsame Verantwortlichkeit der *Miner* ist abzulehnen.⁴⁴ Die *Miner* können lediglich die Transaktionen zusammenfassen und *Hashwerte* errechnen, aber dabei die entsprechenden Daten nicht verändern, weshalb ihnen für die u. U. enthaltenen personenbezogenen Daten nicht die Verantwortung auferlegt werden kann. Prinzipiell besteht für alle Mitglieder des *Blockchain*-Netzwerks keine Möglichkeit, einzelne Transaktion zu löschen. Der einzelne Nutzer kann keine Transaktionen für andere erstellen oder beeinflussen und ist auch nicht in der Lage, seine eigenen Transaktionen rückwirkend zu bearbeiten.⁴⁵

⁴¹ WikiLeaks: Donate to WikiLeaks, unter: <https://shop.wikileaks.org/donate#db3> (15.10.2018).

⁴² Eduard Hofert: Blockchain-Profilung – Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke, in: ZD – Zeitschrift für Datenschutz, 7/4 (2017), S. 161 – 165.

⁴³ Buchner und Kühling: Datenschutz-Grundverordnung, (wie Anm. 34).

⁴⁴ Jörn Erbguth, Joachim Fasching: Wer ist Verantwortlicher einer Bitcoin-Transaktion?, in: ZD – Zeitschrift für Datenschutz ZD Heft 7/12 (2017), S. 12/2017, S. 560 – 565.

⁴⁵ Martini und Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, (wie Anm. 39).

Die DS-GVO normiert in Art. 16 S. 1 und 17 Abs. 1 diverse Rechte, die betroffene Personen gegenüber den Verantwortlichen in Bezug auf ihre personenbezogenen Daten geltend machen können. Im Hinblick auf die Unveränderbarkeit der *Blockchain* lässt sich hier das größte Konfliktpotenzial vermuten. Zunächst normiert Art. 16 S. 1 DS-GVO das Recht betroffener Personen, von dem Verantwortlichen unverzüglich die Berichtigung der die Personen betreffenden, unrichtigen Daten zu verlangen. Dieses Berichtigungsrecht ist für den Betroffenen essenziell, da unrichtig gespeicherte Daten Einfluss auf Entscheidungen wie beispielsweise eine Kreditvergabe haben können. Auch scheinbar bedeutungslose Unrichtigkeiten sind von diesem Recht erfasst, da keine Prognose getroffen werden kann, ob diese künftig nicht noch Relevanz entfalten.⁴⁶ Einträge in der *Blockchain* können nachträglich nicht mehr verändert werden. Art. 16 S. 1 DS-GVO steht somit im vollkommenen Gegensatz zu den eigentlich unveränderlichen Transaktionsdaten, und es bedarf spezieller technischer Implikationen, um ein solches Recht praktisch umzusetzen.

Art. 17 Abs. 1 DS-GVO regelt das Recht auf Löschung in bestimmten Fällen. Demnach dürfen die Daten nur solange gespeichert werden, wie sie auch tatsächlich benötigt werden. Sobald der jeweilige Zweck, für den die Daten verarbeitet wurden, erfüllt ist, sind die Betroffenen berechtigt, die Löschung der Daten zu verlangen. Der Verantwortliche hat also sicherzustellen, dass ein Zugriff auf die Daten nicht mehr oder nur noch mit unverhältnismäßig hohem Aufwand möglich ist. Allerdings lässt sich einer derartigen Aufforderung technisch nur schwer nachkommen, da so auch sämtliche *Hashwerte* ungültig und damit die gesamte Kette inkonsistent werden würde. Um das Recht auf Löschung zu umgehen, könnte man auch argumentieren, dass gerade in der stetigen Fortschreibung der Transaktionshistorie der Zweck des Netzwerks besteht und ein Recht auf Löschung somit gar nicht zur Anwendung kommen würde.⁴⁷

Es zeigt sich, dass das Datenschutzrecht zwar durchaus Anwendung in einem öffentlichen *Blockchain*-Netzwerk finden kann, allerdings scheint die Umsetzung der Betroffenenrechte in der Praxis als nicht leicht handhabbar. Dazu bedarf es gesonderter Regelungen, wie der Datenschutz in *Blockchain*-Netzwerken anzuwenden ist oder wie technische Implikationen, die die Umsetzung und Wahrung des Datenschutzes gewährleisten, grundsätzlich einzusetzen sind.

⁴⁶ Buchner und Kühling: Datenschutz-Grundverordnung, (wie Anm. 34).

⁴⁷ Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14); Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251 – 1270.

5. Zivilrechtliche Aspekte der *Blockchain*-Technologie am Beispiel von *Smart Contracts*

Eine Anfechtung von Verträgen erfolgt gem. § 143 Abs. 1 BGB durch Erklärung gegenüber dem Anfechtungsgegner und bewirkt nach § 142 Abs. 1 BGB, dass ein Rechtsgeschäft als von Anfang an nichtig anzusehen ist. Für Verträge innerhalb des *Blockchain*-Netzwerks würde dies bedeuten, dass bereits validierte und in den Blöcken gespeicherte Transaktionen bei einer wirksamen Anfechtung rückwirkend als nichtig betrachtet werden müssten. Die Technologie zeichnet sich jedoch gerade durch die Unveränderlichkeit der Transaktionshistorie aus.

Die Wirkung des Rücktritts normiert § 346 Abs. 1 BGB. Demnach sind die empfangenen Leistungen zurück zu gewähren und die gezogenen Nutzungen herauszugeben, wenn sich eine Vertragspartei den Rücktritt vertraglich vorbehalten hat oder ihr ein gesetzliches Rücktrittsrecht zusteht. Es stellt sich die Frage wie eine Rückabwicklung in der *Blockchain* abgebildet werden kann, insbesondere wenn der Verkäufer nicht mitwirkt. So kann in einer *Blockchain* niemand Transaktionen für andere Nutzer erstellen, da es stets des jeweiligen zur Adresse gehörenden Schlüsselpaares bedarf.

Im Übrigen stellt sich die Frage, wie innerhalb eines *Blockchain*-Netzwerks gewährleistet werden kann, dass lediglich berechnete Personen Verträge schließen. Zwar ist bei traditionellen Geschäften ebenfalls nicht ausgeschlossen, dass eine nicht berechnete Person ein solches vornimmt, allerdings birgt die *Blockchain* durch die Unveränderlichkeit meist höhere Hürden in der Rückabwicklung oder Auflösung von Geschäften. So ist ein Rechtsgeschäft beispielsweise schwebend unwirksam, wenn es sich bei einer Vertragspartei um einen Minderjährigen handelt. Zur Wirksamkeit des Rechtsgeschäfts bedarf es dann in diesem Fall gem. § 107 BGB der Einwilligung seines gesetzlichen Vertreters, sofern der Minderjährige nicht lediglich einen rechtlichen Vorteil erlangt. Es ist fraglich, wie eine solche schwebende Unwirksamkeit in einer *Blockchain* abgebildet werden kann, ebenso wie geprüft werden soll, ob ein Minderjähriger Transaktionen ausführt.

Die *Blockchain* ist ein unabhängiges, dezentrales Netzwerk. Daher ist fraglich, wie in diesem Rahmen gewährleistet werden soll, dass Transaktionen nicht einem gesetzlichen Verbot i.S.v. § 134 BGB unterliegen. Da es meist keine zentrale Kontrollinstanz gibt, existiert zunächst auch keine Überprüfung der Transaktionsinhalte. Für diesen Fall könnte man mitunter einen Automatismus im *Blockchain*-Netzwerk einbauen, welcher routinemäßig Transaktionen mit gewissen Gesetzen abgleicht.⁴⁸ Allerdings ist es hierbei meist notwendig, das entsprechende Verbot-

⁴⁸ Schrey und Thalhoffer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).

gesetz auszulegen.⁴⁹ Die *Blockchain* speichert jedoch lediglich feste Parameter und lässt keinen Raum für Auslegungsfragen. Dies führt auch zu Kollisionen mit der Sittenwidrigkeit gem. § 138 BGB. Ob Sittenwidrigkeit vorliegt, wird meist unterschiedlich beurteilt und kann somit nur schwer durch Automatismen geprüft werden.⁵⁰ Dies wirft die Frage auf, ob und wie in einem *Blockchain*-Netzwerk juristische Terminologie wie Treu und Glauben, Ermessen, Unzumutbarkeit oder auch höhere Gewalt in der Zukunft Berücksichtigung finden können.⁵¹

6. Lösungsansätze

In diesem Kapitel werden drei exemplarische Lösungsansätze vorgestellt, mit denen die oben angesprochenen Probleme zumindest ansatzweise behoben werden können. Die sog. *Reverse Transactions* führen fehlerbehaftete Transaktionen noch einmal umgekehrt aus, wodurch der wirtschaftliche Zustand, der vor der falschen Transaktion bestand, wiederhergestellt wird. Allerdings bleiben dabei sämtliche Transaktionen transparent einzusehen.⁵²

Beim sog. *Pruning* handelt es sich um die teilweise Löschung bereits vergangener Transaktionen durch eine zentrale Instanz. Dabei ist zu beachten, dass die Daten, die gelöscht werden sollen, bereits wieder in einer neuen Transaktion erhalten sein müssen. Dieser Vorgang ermöglicht es, Daten zu entfernen, ohne den Nachweis über die jeweilige Legitimation zu verlieren und die *Blockchain* weiterzuführen. Dadurch wird die Funktionsfähigkeit der gesamten *Blockchain* bewahrt, da der *Hashwert* des Blocks nicht verändert wird. Dies führt jedoch aller Wahrscheinlichkeit nach zu einem Verlust der Nachvollziehbarkeit und Fälschungssicherheit.⁵³

Die Nutzung des *Chameleon Hashs* ermöglicht es, die eigentliche Unveränderbarkeit, die der *Blockchain*-Technologie zugrunde liegt, zu umgehen, indem Änderungen an bereits verifizierten Transaktionen erlaubt werden. Allerdings erfordert diese Implementierung den Einsatz einer zentralen Instanz, welche nach bestimmten Parametern Löschungen vornimmt und dafür die Zuständigkeit innehat.⁵⁴

⁴⁹ Otto Palandt: Kommentar zum Bürgerlichen Gesetzbuch, 77. Auflage, München 2018.

⁵⁰ Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).

⁵¹ Breidenbach und Gatz: Rechtshandbuch Legal Tech, (wie Anm. 4).

⁵² Schrey und Thalhofer: Rechtliche Aspekte der Blockchain, (wie Anm. 14).

⁵³ Mario Martini und Quirin Weinzierl: Die Blockchain-Technologie und das Recht auf Vergessenwerden, in: NVwZ – Neue Zeitschrift für Verwaltungsrecht 26/17 (2017). S. 1251–1270.

⁵⁴ Ebd.

7. Fazit

»Es gibt destruktive Revolutionen, die das Bestehende angreifen. Und es gibt produktive Revolutionen, die den Weg über das Neue gehen und eben dadurch versuchen, das Alte überflüssig zu machen.«⁵⁵ Bereits im Jahre 2015 veröffentlichte das World Economic Forum eine Studie, die prognostizierte, dass bis zum Jahre 2025 bereits 10 % des weltweiten Bruttoinlandsproduktes mithilfe der *Blockchain*-Technologie generiert werden.⁵⁶

Darüber hinaus soll die *Blockchain*-Technologie es ermöglichen, u. a. Korruption zu umgehen, indem man Transaktionen direkt miteinander, ohne eine dritte Instanz, tätigt. Doch sind u. U. potenzielle Nutzer in Ländern mit hoher Korruptionsquote oder schwacher Infrastruktur noch nicht in der Lage, die Voraussetzungen für die Teilnahme an einem *Blockchain*-Netzwerk, wie einen PC mit entsprechender Internetgeschwindigkeit, zu nutzen.

Weltweit besitzen heutzutage noch immer fast 1,7 Milliarden Menschen keinen Zugang zu einem Bankkonto, dennoch ist die Mehrheit dieser Menschen im Besitz eines Mobiltelefons.⁵⁷ Dieses Ungleichgewicht versucht sich die *Libra Association* zunutze zu machen, zu deren Mitgliedern u. a. Facebook, Uber oder PayPal gehören, indem eine eigene digitale Währung namens *Libra* auf Basis eines *Blockchain*-Netzwerkes etabliert werden soll. Auf diese Weise soll Zugang zu einer einfachen globalen Währungs- und Finanzinfrastruktur für Milliarden von Menschen geschaffen werden, unabhängig von Wohnort, Tätigkeit oder Einkommen. Es handelt sich dabei aktuell jedoch nicht um ein öffentlich zugängliches *Blockchain*-Netzwerk, sondern um ein genehmigungspflichtiges, welches binnen fünf Jahren öffentlich werden soll. Das Mining wird zunächst nur durch die Mitglieder der *Libra Association* betrieben.⁵⁸ Die drohende Konkurrenz scheint dem Kurs der Kryptowährung *Bitcoin* hingegen nicht zu schaden, seit April dieses Jahres steigt der Kurs wieder an. Aktuell ist ein *Bitcoin* rund 9.389 Euro wert.

Für die derzeitigen rechtlichen Herausforderungen im Hinblick auf die *Blockchain*-Technologie lässt sich festhalten, dass es zumindest Lösungsansätze für die

⁵⁵ Milosz Matuschek: Blockchain – eine Technologie revolutioniert unser ganzes Denken, unter: <https://www.nzz.ch/meinung/kommentare/new-kids-on-the-blockchain-ld.1319020> (02.10.2017).

⁵⁶ World Economic Forum: Deep Shift – Technology Tipping Points and Societal Impact, unter: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (01.09.2015).

⁵⁷ World Bank Group: The Global Findex Database 2017 Measuring Financial Inclusion and the Fintech Revolution, unter: <http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf> (01.09.2017).

⁵⁸ Libra Association: White Paper – An Introduction to Libra, unter: https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf (05.05.2019).

Problematiken gibt, wenn auch nicht alle Hürden ohne Weiteres zu bewältigen sind. Inwieweit diese die Integrität beeinflussen oder der eigentlichen Anwendung abträglich sind, hängt von den Intentionen der Anwender im jeweiligen Einsatzgebiet ab und welche Ziele damit verfolgt werden sollen. Es bedarf keinen neuen gesetzlichen Regelungen, sondern einer entsprechenden Auslegung in Bezug auf die *Blockchain*-Technologie und der Entwicklung von Ausnahmen, wie die Akzeptanz von *Reverse Transactions* zur Erfüllung der Rückabwicklung von einem anfechtbaren Rechtsgeschäft.

Auch aufseiten des Gesetzgebers bleibt abzuwarten, ob nicht noch entsprechende rechtliche Rahmenbedingungen für die *Blockchain*-Technologie geschaffen werden, so wie sie in anderen Ländern bereits implementiert wurden. Die CDU/CSU und die SPD haben in ihrem Koalitionsvertrag bestimmt, wie sie sich in Bezug auf die *Blockchain*-Technologie aufstellen wollen. Darin heißt es u. a., dass sie »eine umfassende Blockchain-Strategie entwickeln und sich für einen angemessenen Rechtsrahmen für den Handel mit Kryptowährungen und Tokens auf europäischer und internationaler Ebene einsetzen wollen.« Ferner sollen »innovative Technologien wie Distributed Ledger erprobt werden und basierend auf diesen Erfahrungen ein Rechtsrahmen geschaffen werden.«⁵⁹

Aber nicht nur auf nationaler Regierungsebene wird die Technologie weiter erforscht. Auch auf europäischer Ebene wurde mit der Europäischen Blockchain-Partnerschaft eine Institution geschaffen, welche in verschiedene Projekte investieren möchte, welche die Nutzung der *Blockchain* unterstützen und fördern.⁶⁰ Mitglieder sind nicht nur EU-Mitgliedstaaten, sondern auch einige Mitglieder des europäischen Wirtschaftsraums. Ziel ist es, eine europäische *Blockchain*-Infrastruktur aufzubauen, welche die Bereitstellung grenzüberschreitender digitaler öffentlicher Dienste mit den höchsten Sicherheits- und Datenschutzstandards bis 2020 unterstützt. Außerdem hat es sich die Europäische Kommission zur Aufgabe gemacht, eine internationale Standardisierung der *Blockchain* zu erreichen.⁶¹

Darüber hinaus hat sie gemeinsam mit dem Europäischen Parlament das European Blockchain Observatory gegründet, welches u. a. *Blockchain*-Initiativen in Europa bündeln und ein transparentes Forum für den Informations- und Mei-

⁵⁹ Deutsche Bundesregierung: Koalitionsvertrag zwischen CDU/CSU und SPD vom 14. März 2018, unter: https://www.bundesregierung.de/Content/DE/_Anlagen/2018/03/2018-03-14-koalitionsvertrag.pdf?__blob=publicationFile&v=6 (14.03.2018).

⁶⁰ Europäische Kommission: Erklärung zur Europäischen Blockchain Partnerschaft, unter: <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership> (10.04.2018).

⁶¹ Europäische Kommission: Blockchain Technologies, unter: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> (05.05.2019).

nungsaustausch schaffen soll. Ferner sollen u. a. Austausch und Debatten zum Thema *Blockchain* gefördert werden.

Darüber hinaus wurde eine neue Interessenorganisation, die Internationale Vereinigung für vertrauenswürdige Blockchain-Anwendungen, kurz INATBA, gegründet.⁶² Ziel der INATBA ist es die Potenziale und Vorteile von *Blockchain* und *Distributed Ledger Technology* auszuschöpfen und Rechtssicherheit, Transparenz und Integrität zu fördern.⁶³ Fraglich ist hierbei jedoch, inwieweit bei dieser Vielzahl an Einrichtungen die Seriosität noch gewährleistet ist. Gerade bei der Initiative INATBA sind aktuell weder Vertreter von *Ethereum* oder *Bitcoin* vertreten.⁶⁴

Es werden aber nicht nur unzählige Institutionen gegründet, die mit *Blockchain* als Schlagwort werben. Es wird auch in den verschiedensten Branchen nach neuen innovativen Einsatzmöglichkeiten für die Technologie gesucht. So hat beispielsweise die österreichische Post nun eine sogenannte *Crypto Stamp* angeboten. Dabei handelt es sich um Briefmarken, die zum einen aus einer realen Papierbriefmarke und zum anderen aus einem virtuellen Gegenpart bestehen. Der virtuelle Teil ist mit der *Ethereum Blockchain* verknüpft und ermöglicht somit Zugang zur Kryptowährung *Ether*.⁶⁵ Ob diese Angebote nun helfen, die *Blockchain* in der Gesellschaft zu etablieren, bleibt fraglich.

Die *Blockchain* soll Vertrauen, Sicherheit und Integrität gewährleisten. Dennoch besteht auch dort ein Sicherheitsrisiko, insbesondere für externe Schnittstellen, welche für das Ein- und Auslesen der Daten benötigt werden. Auch bleibt abzuwarten, ob die verwendeten Algorithmen mit der Zeit überholt werden und inwieweit diese dann noch untereinander kommunizieren können. Der Mangel an Standards im Bereich der *Blockchain*-Anwendungen hat zur Folge, dass die verschiedenen Netzwerke untereinander nicht kompatibel sind. Die Vielzahl an Lösungsansätzen macht es insbesondere für unerfahrene Nutzer schwierig, sich für eine bestimmte Anwendung zu entscheiden.⁶⁶

⁶² Europäische Kommission: Launch of the International Association of Trusted Blockchain Applications – INATBA, unter: <https://ec.europa.eu/digital-single-market/en/news/launch-international-association-trusted-blockchain-applications-inatba> (05.05.2019).

⁶³ Europäische Kommission: Blockchain Technologies, unter: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> (05.05.2019).

⁶⁴ Block-Builders: INATBA startet: Verband für Blockchains mit Ripple, IOTA und Cardano an Bord, unter: <https://block-builders.de/inatba-startet-verband-fur-blockchains-mit-ripple-iota-und-cardano-an-bord/> (05.05.2019).

⁶⁵ T3n: Die erste Blockchain Briefmarke der Welt gibt's im Onchain-Shop der Österreichischen Post, unter: <https://t3n.de/news/krypto-oesterreichische-post-1172058/> (22.06.2019).

⁶⁶ Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, unter: <https://www.bsi.bund.de/SharedDocs/>

Ferner bleibt fraglich, wie sich im Gegensatz zu den Institutionen und Forschungsideen die Negativschlagzeilen langfristig auf Kryptowährung und infolgedessen womöglich auch auf die *Blockchain*-Technologie auswirken. So wurden mit *Bitcoins* u. a. auch schon Käufe über die Internetplattform *Silk Road* bezahlt. Dabei handelte es sich um eine Verkaufsplattform im *Dark Web*, auf der u. a. Drogen oder Hacker-Software angeboten wurde, welche bei einem Kauf mit *Bitcoins* bezahlt werden konnten. Das *Dark Web* ist nicht über gängige Webbrowser und Suchmaschinen erreichbar. Es handelt sich um ein anonymisiertes Netzwerk.⁶⁷ Allerdings werden sich diese Probleme auf der einen Seite bei einem öffentlich zugänglichen Netzwerk ohne Kontrollinstanz oder Zugangsvoraussetzungen niemals vermeiden lassen. *Silk Road* war nur ein Beispiel für eine Vielzahl illegaler Plattformen im Internet. Erfolgt keinerlei Kontrolle, lässt sich vermuten, dass auch über öffentliche *Blockchain*-Anwendungen illegale Geschäfte getätigt werden oder deren Bezahlung weitestgehend anonym über Systeme wie *Bitcoin* vorgenommen werden.

In jedem Fall bleibt auch in Zukunft noch zu untersuchen, inwieweit die Daten einer *Blockchain* in der realen Welt valide sind. Die Unveränderbarkeit der Daten in der *Blockchain* garantiert nicht zeitgleich auch die Validität der Daten außerhalb der *Blockchain*.⁶⁸

In welche Richtung die *Blockchain*-Technologie steuert, ist derzeit noch nicht abzusehen. Die Technologie bedarf noch einiger Weiterentwicklung, und es wird sich erst in Zukunft herauskristalisieren, ob die angekündigte Revolution durch die *Blockchain*-Technologie tatsächlich eintritt und langfristig Bestand haben wird. In jedem Fall ist aber bei der Vielzahl an Angeboten Vorsicht geboten. Viele Anbieter und Institutionen möchten u. U. von dem Hype um *Blockchain* profitieren, haben letztlich aber kaum Berührungspunkte damit. Nicht überall, wo *Blockchain* draufsteht, ist auch *Blockchain* drin.

Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5 (05.05.2019).

⁶⁷ Frankfurter Allgemeine Zeitung: Höchststrafe für den Silk Road-Gründer, unter: <https://www.faz.net/aktuell/gesellschaft/kriminalitaet/lebenslange-haft-hoehchststrafe-fuer-den-silk-road-gruender-13620148.html> (30.05.2015).

⁶⁸ Bundesamt für Sicherheit in der Informationstechnik: Blockchain sicher gestalten – Konzepte, Anforderungen, Bewertungen, unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5 (05.05.2019).

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 *Initial 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 Technikiniversitäten, 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, registriert 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 derzeit⁷ 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* vorgebracht 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-Ökologie⁹, 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 beschäftigen. 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 Aufschwimmen 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, unlöschar 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 Technologieverbands, 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 arbeitsbeweismbasierte 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 wurde¹⁷, 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 Verfahren 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* Konsenses¹⁹ 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*-²¹Protokolle 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 Netzwerkknotten 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 Knotten 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-Equilibrium²⁵, 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 Knotten 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 Knotten, die als erstes einen neuen korrekten Block errechnen haben, diesen Block geheim halten und sich damit einen Vorteil gegenüber den anderen Knotten verschaffen, die weiterhin nach diesem Block suchen, während der Knotten, der den richtigen Block schon gefunden hat, bereits den nächsten suchen kann.²⁶ Da sich in der Realität Knotten, 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 Knotten. 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-berüchtigte *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 juristischen 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 Maschinenverbände, 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.

Abstracts

Hermann Kappelhoff: Front Lines of Community: A Postscript to Hollywood War Cinema

What kind of world emerges as a common world for the spectator in the staging of the events of war? And how can the film-analytical reconstruction of a sense of commonality open up historical consciousness in the first place? Focusing on the combat report *WITH THE MARINES AT TARAWA* (USA 1944) this text shows how the ramifications of genre poetics can be explored as a network of experiential modalities that make history graspable as a continuous process of delineating the limits of community.

Anne Eakin Moss: The Camera Shot and the Gun Sight

This article examines the connections between the camera shot and the gun sight in the age of classic Hollywood cinema. Comparing *THE LOST PATROL* (USA 1934, John Ford) with *TRINADTSAT* (*THIRTEEN*, UdSSR 1936, Mikhail Romm), it asks what kind of relationship films from this era strove to establish between the viewer and the gun shot on screen. The ideological and stylistic differences between the films make visible divergent fantasies of agency, community and technology.

Eva Schauerte: Von Delphi zum ORAKEL. Eine kleine Mediengeschichte der Computer-Demokratie

1971 geht mit dem ORAKEL im WDR ein Sozialexperiment auf Sendung, mit dem die partizipative Demokratie mithilfe der neuen Medien – Telefon, Fax, Fernsehen und Com-

puter – erprobt werden soll. Konzipiert von Helmut Krauch, der mit der Heidelberger Studiengruppe für Systemforschung seit Beginn der 1960er Jahre Zukunftsforschung auch im Auftrag der Bundesregierung betreibt, orientiert sich das ORAKEL an der von RAND-Forschern in den USA entwickelten Delphi-Methode. Krauch zufolge stellt das Format einen ersten Schritt auf dem Weg in eine Computer-Demokratie dar, deren kurze Geschichte hier nachgezeichnet wird.

In 1971, the WDR broadcasts the show ORAKEL as a social experiment to test participatory democracy using the new media – telephone, fax, television and computer. Developed by Helmut Krauch, who has been conducting futures studies on behalf of the German government with the Heidelberg Study Group for Systems Research since the early 1960s, ORAKEL is based on the Delphi method developed by RAND researchers in the United States. According to Krauch, the format represents a first step on the way towards a computer democracy, the short history of which is traced in this article.

Debatte: Computeranalphabetismus

In Bildungspolitischen Debatten wird nicht erst seit heute gefordert, so etwas wie eine ›digitale Bildung‹ als neues Unterrichtsfach einzuführen und viele Kultusministerien sind bereits dabei, entsprechende Lehrpläne zu schmieden. Klaus Zierer und Christina Schatz warnen davor, dieser Forderung umgehend und umfassend zu folgen. Die Auswertung einer großen Anzahl an empirische Studien und Metastudien zum Thema habe ergeben, dass die Wirksamkeit von digitalen Medien

auf die Lernleistungen im Durchschnitt nur mäßige Effekte hat. Die elementaren Kulturtechniken Lesen und Schreiben sind mit Papier und Bleistift bzw. dem Buch in der Hand deutlich effektiver zu erlernen als am Laptop oder Tablet. Medien, ob digital oder analog, sind Hilfsmittel des Unterrichts. Entscheidend für den Lernerfolg ist und bleibt die Professionalität von Lehrpersonen. Setzen Lehrpersonen Technik um der Technik willen ein, was derzeit nicht selten zu beobachten ist, zeigen empirische Studien, dass digitale Medien sogar zu negativen Effekten führen können. Infolgedessen wird bei Fragen des Lernens klar: Auf dieser Ebene gelingt eine Revolution nicht durch die digitale Technik.

Heiko Christians ist dagegen überzeugt, dass es den Begriff einer ›digitalen Bildung‹ erst gar nicht geben kann. Wiederholtes Lesen kanonischer Texte – als kulturtechnische Voraussetzung von Bildung – ist heute ein kontraintuitiver, älterer Gebrauch neuester technischer Infrastrukturen. Dieser Gebrauch ist per se nach wie vor nicht ausgeschlossen, aber er ist so unwahrscheinlich wie noch nie. Und er ist überhaupt nur noch so lange möglich oder in geringem Maße wahrscheinlich, wie man diese Gebrauchsweise, die offensichtlich aus anderen, heute ›überwundenen‹ Infrastrukturen und Epochen stammt, im Gedächtnis und in den eingeübten Reflexen der User noch bereit hält und plausibel macht. Genau das aber wäre tatsächlich die Aufgabe von Bildungsinstitutionen, wenn sie ihren alten Bildungsauftrag noch ausführen wollten. Dieselben Institutionen, die sich einmal vornehmlich der Pflege verschiedener kanonischer Textcorpora widmeten, sollen heute ihre Insassen aber nicht mehr bilden, sondern ›fit‹ machen für die ›digitale Zukunft‹. Das heißt präzise, es sollen keine merklichen Unterschiede mehr zwischen den technischen Verhältnissen innerhalb und außerhalb der Institutionen herrschen. Bleibt die Frage, ob man Techniken und Werke aus dieser alten Buchkultur bewahren möchte oder ob Bil-

dung heute ganz anders definiert werden soll?

In education policy debates, there has been a call not only since today to introduce something like ›digital education‹ as a new school subject and many ministries of education are already in the process of forging corresponding curricula. Klaus Zierer and Christina Schatz caution against following this demand immediately and in its entirety. The evaluation of a large number of empirical studies and meta-studies on the subject revealed that the effectiveness of digital media on learning outcomes had only moderate effects on average. The elementary cultural techniques of reading and writing can be learned much more effectively with paper and pencil or a book in hand than on a laptop or tablet. Media, whether digital or analogue, are teaching aids. The professionalism of teachers is and remains decisive for learning success. If teachers use technology for the sake of technology, which is currently not uncommon, empirical studies show that digital media can even lead to negative effects. As a result, when it comes to questions of learning, it becomes clear that a revolution at this level will not succeed through digital technology.

Heiko Christians, on the other hand, is convinced that the term ›digital education‹ cannot exist in the first place. Today, repeated reading of canonical texts – as a cultural precondition for education – is a counterintuitive, old usage of the latest technical infrastructures. This use is still not excluded per se, but it is more improbable than ever before. And it is only possible at all as long as this use, which obviously originates from other infrastructures and epochs that have been ›overcome‹ today, is maintained in the user's memory and in their trained reflexes and constantly made plausible. This, however, is precisely what educational institutions would have to do if they still wanted to carry out their old educational mission. The same institutions that once devoted themselves primar-

ily to the maintenance of various canonical text corpora are today no longer supposed to educate their inmates, but to make them ›fit for the ›digital future‹. In short, this means that there should no longer be any noticeable differences between the technical conditions inside and outside the institutions. The question remains whether one wants to preserve techniques and works from this old book culture or whether education should be defined quite differently today?

Catherine Malabou: Kryptowährungen oder die anarchistische Wende des zeitgenössischen Kapitalismus

John McAfee hat eine Unabhängigkeitserklärung der Währungen (*Declaration of Currency Independence*) verfasst, in der er proklamiert, dass die Zeit gekommen sei, das Staatsmonopol der Herstellung von Devisen und der Kontrolle ihrer Flüsse in Frage zu stellen und das Band zwischen Geographie und Währung aufzulösen. Die Philosophin Catherine Malabou erläutert in ihrem Artikel die ökonomischen und philosophischen Hintergründe ihrer Entscheidung, diese Erklärung zu unterzeichnen.

John McAfee has drafted a *Declaration of Currency Independence* in which he proclaims that the time has come to question the state monopoly on the production and control of foreign exchange and its flows and to break the link between geography and currency. In her article, philosopher Catherine Malabou explains the economic and philosophical background leading to her decision to sign this declaration.

Rüdiger Weis: Vertrauen aus Mathematik

In Zeiten, in denen jahrzehntelang stabile Vertrauensverhältnisse global immer stärker erschüttert werden, suchen die Menschen nach neuen Vertrauensansätzen. Die libertäre Philosophie hinter *Bitcoin* nutzt einfache und

verständliche Techniken aus der Mathematik, um ein Währungssystem ohne Banken und Staaten zu schaffen. Durch die Geschwindigkeit und die weltweite Verfügbarkeit von Kommunikationsnetzen findet somit ein völlig neuartiges gesellschaftliches Experiment statt.

In times in which stable relationships of trust have been increasingly shaken around the globe for decades, people are looking for new approaches to the ability to trust. The libertarian philosophy behind Bitcoin uses simple and understandable mathematical techniques to create a monetary system without banks and states. The speed and worldwide availability of communication networks thus make for a completely new social experiment.

Stefan Münker: Freiheit, die in Ketten liegt. Eine Philosophie der Blockchain

Die dezentrale Technologie der *Blockchains* verspricht durch ihre spezifische Netzwerk-Architektur ihren Nutzern sowohl mehr Freiheit und Autonomie als auch mehr Sicherheit und Transparenz. Damit wurden *Blockchains* in den letzten Jahren zur Projektionsfläche demokratischer und egalitärer Utopien. Der Beitrag ist eine medienphilosophische Analyse der Idee der *Blockchain* und ihrer praktischen Umsetzungen und zielt auf eine kritische Prüfung der mit *Blockchains* verbundenen Versprechen und Erwartungen.

The decentralized technology of blockchains promises its users more freedom and autonomy as well as more security and transparency through its specific network architecture. In recent years, blockchains have thus become a projection screen for democratic and egalitarian utopias. The contribution is a media-philosophical analysis of the Blockchain idea and its practical implementation and aims at a critical examination of the promises and expectations associated with Blockchains.

Jan Claas van Treeck: Ketten des (Miss-) Vertrauens. Über die Blockchain, Bitcoins und Verwandtes

Die *Blockchain* ist den Weg aus der technischen Obskuranz über eine weitgehend abgeklungene Phase der utopisch-mystifizierenden Begeisterung hin zu etablierten Branchenlösungen gegangen. Blockchainbasierte Kryptowährungen sind längst anerkannte und langsam auch institutionell genutzte Zahlungsmittel. Trotzdem scheinen sich Blockchain-Lösungen immer noch eher über ein Versprechen zu verkaufen, das ein soziales Bedürfnis – das des Vertrauens innerhalb von Systemen – befriedigen will. Ein Blick auf die Technizitäten der Blockchain jedoch erlaubt Einsichten in die Möglichkeit solcher technosozialer Versprechen und ihrer (Nicht-) Einlösbarkeit.

Blockchain has found its way out of technical obscurity via a largely faded phase of utopian-mystifying enthusiasm to established industry solutions. Blockchain-based crypto currencies have long been accepted as a means of payment and are tentatively being used institutionally as well. Nevertheless, Blockchain solutions still seem to sell a promise that seeks to satisfy a social need—that of trust within systems. A glance at the technicalities of Blockchain, however, allows insights into the possibility of such techno-social promises and their (non-)redeemability.

Cathrin Hein, Christoph Hein, Wanja Wellbrock: Hype oder Horror – Potenziale und Hürden der Blockchain-Technologie anhand rechtlicher Rahmenbedingungen

Dieser Beitrag fasst den aktuellen Stand der rechtlichen Herausforderungen der *Blockchain*-Technologie kurz und prägnant zusammen. *Blockchain* stellt, ähnlich dem *World Wide Web*, eine Art Grundlagentechnologie dar, auf deren Basis neue Plattformen und Geschäftsmodelle geschaffen wer-

den können. Es stellt sich jedoch die Frage, ob das deutsche Rechtssystem grundsätzlich in der Lage ist, die Herausforderungen, die eine solch dezentrale Technologie mit sich bringt, zu bewältigen. Insbesondere hinsichtlich strafbarer Handlungen oder der neuen Datenschutzgrundverordnung. Fraglich ist dabei, wie sich die derzeitigen Negativschlagzeilen (beispielsweise *Silk Road*) langfristig auf Kryptowährungen und infolgedessen womöglich auch auf die *Blockchain*-Technologie, nicht nur im Hinblick auf die rechtswidrigen Inhalte wie Kinderpornographie, auswirken.

This article summarizes the current status of the legal challenges of *blockchain* technology. Similar to the *World Wide Web*, *Blockchain* represents a kind of basic technology on the basis of which new platforms and business models can be created. However, the question arises as to whether the German legal system is fundamentally capable of mastering the challenges posed by such a decentralized technology. In particular with regard to criminal offences or the new Basic Data Protection Ordinance. The question is how the current negative headlines (e. g. *Silk Road*) will affect crypto currencies in the long term and, as a result, *blockchain* technology, not only with regard to illegal content such as child pornography.

Oliver Leistert: Kontrolle ist gut, Vertrauen ist besser, Bezahlung am besten: zur Souveränität von Blockchains

Dezentrale, offene *Blockchain*-Technologien verwalten auf protokologischer Ebene Transaktionen von Daten. Durch kryptographische Methoden lassen sich die Transaktionen der Daten identifizieren. Dies geschieht – wenn kein Softwareupdate erfolgt – ohne Eingriff von aussen. Deshalb werden Blockchains als souveräne Medientechnologien vorgestellt. Sie regieren sich selbst. Damit sind sie auf Kollisionskurs mit traditionellen Souveränitäten, die entscheiden dürfen, was der Fall ist.

Zu beobachten ist deshalb das Auftreten einer generisch digitalen Souveränitätsform. Deren Konsensfindung über den Zustand ihres Regierungsbereichs wird analysiert.

Decentralized, open *blockchain* technologies manage transactions of data on a protocological level. Cryptographic methods can be used to identify data transactions. This happens—if no software update takes place—without ex-

ternal intervention. *Blockchains* are therefore presented as sovereign media technologies. They govern themselves. This puts them on a collision course with traditional sovereignties that are allowed to decide what is the case. The emergence of a generic digital form of sovereignty can therefore be observed. Their consensus on the state of their government will be analyzed.

Autorenangaben

Heiko Christians ist Professor für Medienkulturgeschichte an der Universität Potsdam. Arbeitsschwerpunkte: Mediengebrauchsgeschichte, Medienpathologien, Neuer Deutscher Film (1960-1980), Geschichte des Medienkonsums. Ausgewählte Veröffentlichungen: *Crux Scenica. Eine Kulturgeschichte der Szene von Aischylos bis YouTube* (Bielefeld 2016); *Amok. Geschichte einer Ausbreitung* (Bielefeld 2008); *Der Traum vom Epos. Romankritik und politische Poetik in Deutschland 1750 – 2000* (Freiburg 2004).

Cathrin Hein ist Unternehmensberaterin. Arbeitsschwerpunkte: datenschutzrechtlichen Fragestellungen. Ausgewählte Veröffentlichungen: zus. mit Christoph Hein und Wanja Wellbrock: *Rechtliche Herausforderungen von Blockchain-Anwendungen* (Wiesbaden 2018).

Christoph Hein ist Unternehmensberater mit dem Schwerpunkt Digitalisierung von Geschäftsprozessen und der Analyse von Unternehmensdaten. Arbeitsschwerpunkte: Industrie 4.0, Big Data, Predictive und Prescriptive Analytics. Ausgewählte Veröffentlichungen: zus. mit Cathrin Hein und Wanja Wellbrock: *Rechtliche Herausforderungen von Blockchain-Anwendungen* (Wiesbaden 2018).

Hermann Kappellhoff, Film- und Medienwissenschaftler, ist Professor für Filmwissenschaft an der Freien Universität Berlin und leitet zusammen mit Michael Wedel die Kolleg-Forschungsgruppe »Cinopoetics – Poetologien audiovisueller Bilder«. Arbeitsschwerpunkte: Mediale Emotionen und Affektpoetiken, Ästhetik und Politik audiovisueller Bilder,

Genre und Geschichte. Veröffentlichungen: *Kognition und Reflexion: Zur Theorie filmischen Denkens* (Berlin/Boston 2018); zus. mit Cornelia Müller: *Cinematic Metaphor: Experience – Affectivity – Temporality* (Berlin/Boston 2018); *Front Lines of Community: Hollywood Between War and Democracy* (Berlin/Boston 2018).

Oliver Leistert ist wissenschaftlicher Mitarbeiter an der Leuphana Universität Lüneburg. Arbeitsschwerpunkte: digitale Kulturen, Medienkultur und Machtanalytiken, sowie Medienphilosophie. Ausgewählte Veröffentlichungen: zus. mit Lina Dencik: *Critical Perspectives on Social Media and Protest* (London 2015); *From Protest to Surveillance – The Political Rationality of Mobile Media: Modalities of Neoliberalism* (Frankfurt am Main 2013).

Catherine Malabou ist Professorin für Philosophie am Centre for Research in Modern European Philosophy der Kingston University und an der European Graduate School. Arbeitsschwerpunkte: Ästhetik, Psychoanalyse, Neurowissenschaft, Plastizität. Ausgewählte Veröffentlichungen: *Was tun mit unserem Gehirn?* (Zürich/Berlin 2006); *Ontologie des Akzidentiellen. Essay zur zerstörerischen Plastizität* (Berlin 2011); *Before Tomorrow. Epigenesis and Rationality* (Cambridge/Malden, MA 2016).

Anne Eakin Moss is an Assistant Professor at The Johns Hopkins University Department of Comparative Thought and Literature. Main focuses of research: Russian and Soviet literature and cinema, film and media studies.

Selected Publications: *Only Among Women: Philosophies of Community in the Russian and Soviet Imagination, 1860-1940* (Evanston, IL 2019).

Stefan Münker ist Privatdozent an der Humboldt-Universität zu Berlin. Arbeitsschwerpunkte: Theorie und Philosophie (vor allem) digitaler Medien, Geschichte und Philosophie des Fernsehens. Ausgewählte Veröffentlichungen: *Philosophie nach dem »Medial Turn«* (Bielefeld 2009); *Emergenz digitaler Öffentlichkeiten* (Frankfurt am Main 2009); zus. mit Alexander Roesler (Hg.): *Was ist ein Medium?* (Frankfurt am Main 2008)

Christina Schatz ist Wissenschaftliche Mitarbeiterin am Lehrstuhl für Schulpädagogik der Universität Augsburg. Arbeitsschwerpunkte: empirische Bildungsforschung, Unterrichtsqualität aus Sicht der Lernenden. Ausgewählte Veröffentlichungen: zus. mit Klaus Zierer: *Digitalisierung erfordert Professionalisierung! Warum eine Digitalisierung im Schulkontext in entscheidender Weise von der Lehrerprofessionalität abhängt, in: Schulverwaltung Bayern. Fachzeitschrift für Schulentwicklung und Schulmanagement* 41/11 (2018), S. 292–296.

Eva Schauerte ist wissenschaftliche Mitarbeiterin am Internationalen Kolleg für Kulturtechnikforschung und Medienphilosophie (IKKM) der Bauhaus-Universität Weimar. Arbeitsschwerpunkte: Medienphilosophie, Kulturtechniken, Mediale Historiographien, Mediengeschichte der Computer-Demokratie. Ausgewählte Veröffentlichungen: *Lebensführungen. Eine Medien- und Kulturgeschichte der Beratung* (Paderborn 2019); zus. mit Sebastian Vehlken (Hg.): *Faktizitäten. Zeitschrift für Medienwissenschaft* 19 (2018).

Jan Claas van Treeck ist Wissenschaftlicher Mitarbeiter am Institut für Musikwissenschaft

und Medienwissenschaft der Humboldt-Universität zu Berlin. Arbeitsschwerpunkte: Kybernetik, Operativität und Mensch-Maschine-Verschmelzungen. Ausgewählte Veröffentlichung: zus. mit Stefan Höltgen (Hg.): *Time to Play: Zeit und Computerspiel* (Glückstadt 2016).

Rüdiger Weis, Mathematiker, ist Professor für Systemprogrammierung an der Beuth Hochschule für Technik Berlin und Gründer des gemeinnützigen Vereins »Digitale Gesellschaft«. Arbeitsschwerpunkte: Kryptographie, Computersicherheit und Betriebssysteme. Ausgewählte Veröffentlichungen: *A Protocol Improvement for High-Bandwidth Encryption Using Non-Encrypting Smart Cards* (Amsterdam 1999); *Secure and Reliable Firewall Systems Based on MINIX 3* (Amsterdam 2016); *Technische Sicherung der Digitalen Souveränität* (Wiesbaden 2016).

Ines Weizman ist Juniorprofessorin für Architekturtheorie an der Bauhaus-Universität Weimar, Direktorin des Bauhaus-Instituts für Geschichte und Theorie der Architektur und Planung und Direktorin des Centre for Documentary Architecture (CDA). Arbeitsschwerpunkte: Dokumentarische Architektur, digitale Historiographien, Exilgeschichte der Architektur der Moderne, Architektur und Dissidenz. Ausgewählte Veröffentlichungen: (Hg.): *Architecture and the Paradox of Dissidence* (London, 2014); zus. mit Eyal Weizman: *Before and After: Documenting the Architecture of Disaster* (Moskau/London, 2014); (Hg.): *Dust & Data. Traces of the Bauhaus across 100 Years* (Leipzig, 2019).

Wanja Wellbrock ist Professor für Beschaffungswirtschaft an der Hochschule Heilbronn und dort zusammen mit Daniela Ludin leitend für den Studiengang »Nachhaltiges Beschaffungsmanagement« zuständig. Arbeitsschwerpunkte: Big Data-Anwendungen im Beschaffungsmanagement, Blockchain-

Lösungen in der Supply Chain, Strategisches und nachhaltiges Beschaffungsmanagement. Ausgewählte Veröffentlichungen: (Hg.): Nachhaltiges Beschaffungsmanagement. Strategien, Praxisbeispiele, Digitalisierung (Wiesbaden 2019); Rechtliche Herausforderungen von Blockchain-Anwendungen. Straf-, Datenschutz- und Zivilrecht (Wiesbaden 2019); Innovative Supply-Chain-Management-Konzepte. Branchenübergreifende Bedarfsanalyse sowie Konzipierung eines Entwicklungsprozessmodells (Wiesbaden 2015).

Klaus Zierer ist Professor für Schulpädagogik an der Universität Augsburg. Arbeitsschwerpunkte: empirische Bildungsforschung, erlebtes Lernen, Digitalisierung in Schule und Unterricht, Visible Learning. Ausgewählte Veröffentlichungen: zus. mit Julian Nidarümelin: Auf dem Weg in eine neue deutsche Bildungskatastrophe. 12 unangenehme Wahrheiten (Freiburg 2015); zus. mit Benedikt Wisniewski: Visible Feedback – Leitfaden für erfolgreiches Unterrichtsfeedback (Baltmannsweiler 2017); zus. mit John Hattie: Visible Learning auf den Punkt gebracht. (Baltmannsweiler 2018).

Adressen Autoren ZMK 10|2|2019

Heiko Christians
Universität Potsdam
Institut für Künste und Medien /
Europäische Medienwissenschaft
Am Neuen Palais 10
14469 Potsdam
hchrist@uni-potsdam.de

Cathrin Hein
Christoph Hein
HENDRICKS, ROST & Cie. GmbH
Cecillienalle 66
40474 Düsseldorf
chein@outlook.com

Hermann Kappelhoff
Freie Universität Berlin
Institut für Theaterwissenschaft
Grünwaldstraße 35
12165 Berlin
sekretariat-kappelhoff@fu-berlin.de

Oliver Leistert
Leuphana Universität Lüneburg
Fakultät Kulturwissenschaften
Universitätsallee 1
21335 Lüneburg
leistert@leuphana.de

Catherine Malabou
Centre for Research in Modern European
Philosophy
Kingston University
Penrhyn Road
Kingston upon Thames
KT1 2EE
c.malabou@kingston.ac.uk

Anne Eakin Moss
The Johns Hopkins University
Department of Comparative Thought and
Literature
3400 N Charles St
Baltimore, MD 21218 USA
aeakinmoss@jhu.edu

Stefan Münker
Humboldt-Universität zu Berlin
Kultur, Sozial- und
Bildungswissenschaftliche Fakultät
Institut für Musikwissenschaft und
Medienwissenschaft
Fachgebiet Medienwissenschaft
Unter den Linden 6
10099 Berlin
stefan.muenker@hu-berlin.de

Eva Schauerte
Bauhaus-Universität Weimar
Internationales Kolleg für
Kulturtechnikforschung und
Medienphilosophie
Cranachstraße 47
99423 Weimar
eva.schauerte@uni-weimar.de

Jan Claas van Treeck
Humboldt-Universität zu Berlin
Institut für Musikwissenschaft und
Medienwissenschaft
Bereich Medienwissenschaft
Georgenstraße 47
10117 Berlin
jc.vantreeck@hu-berlin.de

Rüdiger Weis
Beuth Hochschule für Technik Berlin
Fachbereich VI – Informatik und Medien
Haus Bauwesen, D 131
Luxemburger Str. 10
13353 Berlin
ruediger.weis@beuth-hochschule.de

Ines Weizman
Bauhaus-Universität Weimar
Architektur und Urbanistik
Geschwister-Scholl-Straße 8
99423 Weimar
ines.weizman@uni-weimar.de

Wanja Wellbrock
Hochschule Heilbronn
Fakultät Management und Vertrieb
Ziegeleiweg 4
74523 Schwäbisch Hall
wanja.wellbrock@hs-heilbronn.de

Klaus Zierer / Christina Schatz
Universität Augsburg
Philosophisch-Sozialwissenschaftliche
Fakultät
Universitätsstraße 2
86159 Augsburg
klaus.zierer@phil.uni-augsburg.de
christina.schatz@phil.uni-augsburg.de

Zeitschrift für Medien- und Kulturforschung

Herausgegeben von
Lorenz Engell und Bernhard Siegert

Bisherige Schwerpunkte:

0 (2009) Angst
1|1 (2010) Kulturtechnik
1|2 (2010) Medienphilosophie
2|1 (2011) Offene Objekte
2|2 (2011) Medien des Rechts
3|1 (2012) Entwerfen
3|2 (2012) Kollektiv
4|1 (2013) Medienanthropologie
4|2 (2013) ANT und die Medien
5|1 (2014) Producing Places
5|2 (2014) Synchronisation
6|1 (2015) Textil
6|2 (2015) Sendung
7|1 (2016) Verschwinden
7|2 (2016) Medien der Natur
8|1 (2017) Inkarnieren
8|2 (2017) Operative Ontologien

9|1 (2018) Mediocene
9|2 (2018) Alternative Fakten
10|1 (2019) Ontography
10|2 (2019) Blockchain

Vorschau:

11|1 (2020) Schalten und Walten

Informationen zur *Zeitschrift für Medien- und Kulturforschung* finden Sie unter
www.ikkm-weimar.de/zmk bzw. www.meiner.de/zmk.