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 bekanntermaßen 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 halbfalscher 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 Freunds 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 Verdatung der ersten Welt, genauso ›angeleimt‹ wie das Symbolische der Sprache. Und sowohl das Symbolische der Sprache als auch das operative Symbolische der Verdatung können abgelöst und ›umgeleimt‹ werden, nicht nur in der Gemüseabteilung. Leiht 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' Selbstauskunft 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 ›Technohurrapatrioten‹ 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 vordergründig 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 Befeuerer heute ihren damaligen Technohurrapatriotismus 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/manouchehr-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 dekonditioniert 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 *aus*geführt, 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, Fankfurt am Main 1998, S. 225 f.
13 Nakamoto: Bitcoin (wie Anm. 10).
14 Ebd.

ten Kryptowährungen zeigt sich dann bei genauerem technischen Hinsehen die Nichteinlösbarkeit 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).