# Vom Freiheitsversprechen der Blockchain und seinen Nebenwirkungen

Katrin Becker

„Die Blockchain-Technologie ist in aller Munde“ – dieser Eindruck verfestigt sich, sobald man sich auch nur ansatzweise mit ihr beschäftigt. Die Regierungen von u.a. Deutschland, Frankreich und Italien etablieren Arbeitsgruppen zur Entwicklung einer Blockchain-Strategie, Estland verlegt einen Großteil seiner Verwaltung auf die Blockchain[1] – und auch in Luxemburg soll eine neue Gesetzgebung den Einsatz der Blockchain-Technologie fördern: ein gesetzgeberischer Zug, der als “the start of blockchain technology gaining legal acceptance in one of the most protective regional territories of the world” gehandelt wird.[2] Umso überraschender erscheint es, dass man im privaten Umfeld immer wieder auf Menschen trifft, die noch nie von dem Begriff „Blockchain“ gehört haben.

Worum geht es also bei der Blockchain – und warum ist es, so denke ich, an der Zeit, die Debatte über den Einsatz dieser Technologie und ihre Implikationen nicht allein den Bitcoin-Sammlern, anarchokapitalistischen Technik-Liebhabern und Dezentralisierungsadepten zu überlassen?

## Das Transaktionsinternet

Die Blockchain ist ursprünglich die der Kryptowährung Bitcoin zugrundeliegende Technologie. Sie lässt sich im Grunde genommen als „Transaktionsinternet“ beschreiben, insofern als sie dort, wo das Internet Informationen transportiert, Transaktionen ermöglicht. Im Detail handelt es sich bei der Blockchain um ein öffentliches, dezentrales, digitalisiertes und kryptografisch operierendes Register. Gemäß einem spezifischen konsensbasierten Verfahren werden hier jegliche Transaktionsinformationen auf unlöschbare, für jeden nachvollziehbare und dadurch schließlich fälschungssichere Weise gespeichert: Jede neu hinzukommende Information wird in einem *block* gespeichert, der durch einen sogenannten kryptografischen Hashwert an die vorangegangen *blocks* gekettet ist – die Fälschung eines einzelnen *blocks* würde so die Veränderung der gesamten Blockchain nach sich ziehen. Dieses Register der *blocks* wird kontinuierlich auf sämtlichen an der Blockchain beteiligten, peer-to-peer vernetzten Computern upgedatet. Durch diese dezentrale Speichermethode sowie das spezifische konsensbasierte Rechenverfahren (Proof of Work), das die Validität der neuen Information auf eine für jeden nachvollziehbare Weise bestätigt, fällt die Notwendigkeit eines zentralen Kontrollorgans, des die Vertrauenswürdigkeit garantierenden Dritten, weg.

An dieser Stelle horcht der Kulturtheoretiker unweigerlich auf – denn die Figur des Dritten ist gemäß vieler Kulturtheorien und insbesondere jener *Pierre Legendres*[3] das zentrale Element für die Funktionsfähigkeit und Identitätsbildung des kulturellen, gesellschaftlichen und individuellen Lebens: Es bedarf eines großen Dritten, in dessen Namen Recht gesprochen wird (im Namen Gottes, des Staates, des Volkes) und die Werte und Bedeutungen im zwischenmenschlichen Austausch garantiert werden. Ohne eine zentrale Bankeninstanz, die den Wert des Geldes festsetzt, wäre dieses als Tauschmittel nutzlos; ohne ein Institutionensystem, das eine gemeinschaftliche Sinngrundlage verkörpert, darlegt, was Recht und Unrecht ist, wären ein friedliches Leben und die Verständigung zwischen den Mitgliedern einer Gesellschaft nicht möglich. Eben solcher Instanzen soll es also nun nicht mehr bedürfen, bzw. vielmehr sollen diese abgelöst werden durch den

**Es bedarf eines Dritten, in dessen Namen Recht gesprochen wird.**

Dr. Katrin Becker ist Postdoctoral Researcher an der Universität Luxemburg. Zurzeit lebt und forscht sie als Fellow am Institut d’Études Avancées in Nantes.

**Die Glaubensbindung an eine gemeinschaftliche Sinn- und Institutionsgrundlage ist für das menschliche Zusammenleben in einer Kultur unumgänglich**

algorithmischen Krypto-Code der Blockchain: „Ob Banken, Notenbanken, Notare, Register, Kataster, Großkonzerne, oder in letzter Konsequenz auch staatliche Gebilde: Zentrale Strukturen sind überholt und zu überwinden. Ihre Funktion als Mittler des gesellschaftlichen Zusammenlebens übernimmt die dezentrale Blockchain-Datenbank."[4]

Der unfälschbare und konsensbasierte Code der Blockchain soll das Vertrauen in einen die Richtigkeit der Information garantierenden Dritten überflüssig machen. Es ist die Rede vom *trustless trust*, d.h., es genügt das Vertrauen in den der jeweiligen Blockchain zugrundeliegenden, programmierten Code. Inzwischen gibt es neben der Bitcoin viele weitere Blockchains, die über die monetären Ziele von Kryptowährungen hinausgehen: So ist es insbesondere die Blockchain Ethereum, die es nunmehr ermöglicht, durch den Einsatz sogenannter *smart contracts* – kleiner Computer-Programme, die nach der „wenn-dann"-Logik operieren – rechtsähnliche Strukturen zu schaffen. Durch das Versenden von Beträgen der jeweiligen Kryptowährung oder das Einspeisen einer neuen Information als Bedingung „wenn" tritt eine Code-Veränderung „dann" automatisiert und in Echtzeit ein. Die Einhaltung eines Vertrags muss somit nicht mehr durch dritte Instanzen, wie Anwälte, Notare oder Bänker, abgesichert werden – durch seine Unveränderlichkeit und Vertrauenssicherheit sorgt nunmehr der Blockchain-Algorithmus zuverlässig und automatisch für die Umsetzung der programmierten Vertragsbedingungen.

### Die Befreiung des Subjekts?

Der von den Gründern und Verbreitern angestrebte – und unleugbare – Vorteil der Blockchain besteht darin, das Subjekt aus den Fängen datensammelnder Firmen oder korrupter Staaten zu lösen: Durch die Automatisierung, Fälschungssicherheit und Dezentralisierung von Datenspeicherung und -versand können Geldtransfers, Grundbucheinträge etc. unabhängig von Bank- oder Staatssystemen vollzogen werden; zudem sind direkte peer-to-peer Transaktionen ohne die Einschaltung vermittelnder, profitorientierter Konzerne möglich: Beim Erhalt eines bestimmten Kryptowährungsbetrags springt die Tür zur gemieteten Wohnung auf oder wird die vereinbarte Ware auf das Konto bzw. den Computer des Käufers übertragen.[5] Auf diese Weise wird das Subjekt zugleich wieder Herr über seine Daten: Durch den Wegfall der Bindung an datenverwaltende Dritte, das System des öffentlich-privaten Krypto-Schlüssels und das „zero-knowledge"-Protokoll, das den Nachweis der Richtigkeit einer Information ohne Inhaltsenthüllung ermöglicht, kann es jeweils selbst entscheiden, wem auf welche Daten Zugriff gewährt wird.[6]

Allerdings werden im Enthusiasmus angesichts dieser Souveränitätsgewinne aufseiten des Subjekts zwei Aspekte ausgeblendet, die von zentraler rechts- und kulturtheoretischer Bedeutung sind: Zwar muten die meisten Blockchain-Szenarien mit gesellschaftspolitischem Anspruch bislang unrealistisch, zumindest aber futuristisch an – wie etwa die vom Bitnation-Projekt angestrebte Möglichkeit, dem Subjekt die Gründung eines eigenen Staates bzw. einer "Decentralised Borderless Voluntary Nation" (DBVN) mit eigenen „Verfassungen, ökonomischen Modellen, Rechtscodes"[7] zu ermöglichen. Doch die Vorstellungen von automatisierten und fallweise programmierbaren Rechtsfunktionen, von materielosen Gemeinschaften, personalisierten Verwaltungsdiensten und freiwilligen Nationen haben unweigerlich Auswirkungen auf die Selbst- und Weltwahrnehmung der Subjekte und damit auf die Einstellung gegenüber dem traditionellen – als Dritter fungierenden – Institutionen- und Rechtssystem.[8] Zugleich ist unstreitig, dass die Durchsetzungskraft des Rechts angesichts der globalen und dezentralen Struktur der Blockchain zunehmend prekär wird: „(...) wenn eine ausreichende Zahl an Minern oder Mining Pools in Jurisdiktionen wohnen, die von möglicherweise erlassenen Regulierungen nicht betroffen sind, kann das Blockchain-basierte Netzwerk sich entweder spalten oder weiterlaufen, als würden diese Regulierungen nicht existieren."[9]

Zum anderen blendet der Jubel über die Überwindung des Dritten und den individuellen Souveränitätsgewinn die Frage nach möglichen neuen Zwängen und Abhängigkeiten aus, die sich aus der völligen Überantwortung von Rechts- und Gesellschaftsstrukturen an den Blockchain-Code ergeben. Denn gerade aus der Verknüpfung von Blockchain und dem wachsenden *Internet of Things* scheint dem global und dezentral operierenden Code eine

*Bitcoin* von MichaelWuensch via Pixabay

geradezu gottgleiche Machtposition zu erwachsen: Einmal programmiert, vermag er menschenunabhängig zu operieren und Kontroll- und Steuerungs-, letztlich Straf- und Belohnungsfunktionen zu übernehmen.[10] So liest man in *The Atlantic*, wie es durch den Einsatz automatischer und an Kryptowährung und Smart-contracts angeschlossener Autos im Grunde unmöglich würde, zu „vergessen, die Parkgebühr zu zahlen. Die einzige Versagensmöglichkeit meinerseits wäre, dass mein Auto über keine Bitcoin mehr verfügt, und in dem Fall hätte der Parkplatz eine einfache Regressmöglichkeit: Da die Zündung meines Autos von einem Computer gesteuert wird, könnte der Parkplatz einfach meinen Wagen ausschalten".[11]

## Freiheit mit Risiko

Die Glaubensbindung an eine gemeinschaftliche Sinn- und Institutionsgrundlage ist für das menschliche Zusammenleben in einer Kultur unumgänglich – mit der Blockchain wird dieses Erfordernis nicht abgeschafft, sondern gewandelt in den Glauben an einen programmierbaren Code, dessen Funktionsweise unweigerlich neue Werte, Gesellschafts- und Rechtsstrukturen mit sich bringt. Zwar fallen viele der momentan entstehenden Anwendungsbereiche, wie das blockchainbasierte Speichern von produktspezifischen Lieferketten, staatseigenen Verwaltungssystemen oder verbandsinternen Transaktions-Historien, in die Kategorie der „privaten" oder „hybriden" Blockchains, die durch die Schaffung eines neuen zentralen Kontrollorgans der grundlegenden Dezentralisierungsidee der Blockchain zuwiderlaufen:[12] Doch machen diese eine neue Technologie hoffähig, die gerade aufgrund ihrer vermeintlich Freiheit und Autonomie bringenden Automatisierungs- und Dezentralisierungsmöglichkeiten, welche sich fernab von jeglicher rechtsstaatlicher Zugriffsmöglichkeit programmieren lassen, dringend im Hinblick auf ihre kultur- und rechtstheoretischen Implikationen zu diskutieren ist. ◆

1 https://berlinvalley.com/estland, letzter Aufruf: 13. März 2019

2 https://cryptopotato.com/will-luxembourg-become-the-first-european-nation-to-legalize-blockchain-tech, letzter Aufruf: 7. März 2019

3 Pierre Legendre ist ein Philosoph, Psychoanalytiker und Rechtshistoriker, der ausgehend von der Psychoanalyse Jacques Lacans eine Kulturtheorie unter dem Namen „dogmatische Anthropologie" entwickelt hat, die im Wesentlichen um die Figur des Dritten kreist und ausgehend davon die spezifischen Eigenschaften der (Rechts-)Kultur des Abendlandes nachzeichnet.

4 https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/krypto-kolumne/coin-und-co-die-krypto-kolumne-das-blockchain-manifest-und-seine-abgruende/21245486.html, letzter Aufruf: 7. März 2019

5 Die über den Blockchain-Code ermöglichte algorithmische Verknüpfung verschiedener – autonom und automatisch operierender – *smart contracts* wird fortentwickelt in den sogenannten DAOs (Decentralized Autonomous Organizations): eine Unternehmensform, „deren Statuten, Geschäftsordnung, Gesellschaftsvertrag oder Satzung durch einen Smart Contract abgebildet und automatisch ausgeführt werden. Die Spielregeln der Organisation werden im Vorfeld definiert und in die Smart Contracts programmiert. DAOs brauchen kein zentral organisiertes Managements des Tagesgeschäfts mehr." Shermin Voshmgir, *Blockchains, Smart Contracts und das Dezentrale Web*, https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf, S. 14, letzter Aufruf: 10. März 2019.

6 https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1, letzter Aufruf: 13. März 2019. So gewann gerade den zweiten Platz eines vom deutschen Gesundheitsministerium ausgeschriebenen Ideenwettbewerbs das Projekt der Blockchain-basierten Patienteneinwilligung, durch das „Patienten [..] für jeden Einzelfall Abmachungen treffen können, was mit ihren Daten geschieht – sowohl bei genetischen als auch anderen personenbezogenen Daten." https://www.egovernment-computing.de/potenziale-der-blockchain-im-gesundheitswesen-a-807539, letzter Aufruf: 13. März 2019

7 https://www.blokt.com/news/bitnation-is-blockchain-technology-moving-us-towards-a-post-nation-state-world, letzter Aufruf: 7. März 2019

8 Alain Supiot, *La gouvernance par les nombres. Cours au Collège de France 2012-2014*, Paris, Fayard, 2015, S. 300: Damit dieses seine Gültigkeit und Geltungskraft bewahrt, müssen seine Mitglieder, so der Rechtswissenschaftler Alain Supiot, ihm „Glauben schenken". «Si les gouvernés ne s'y reconnaissent plus, le théâtre tourne au guignol, c'est-à-dire à un spectacle auquel on ne peut plus ni se fier, ni s'identifier.» (Ebd. S. 299). Vgl. hierzu meinen Artikel «La technologie blockchain – ou: Le désir algorithmique de surmonter la nécessité du tiers», in: *Grief. Revue sur les mondes du droit*, 2, 2019, (im Erscheinen).

9 Primavera De Filippi/Aaron Wright, *Blockchain and the Law: The Rule of Code*, Cambridge, Mass., Harvard University Press, 2018, S. 181. In diesem Sinne arbeiten verschiedene Korporationen bereits an Möglichkeiten der Kontrolle, der Anreize oder technischer Einfalltüren für nationalgesetzliche bzw. gemeinschaftsrechtliche Eingriffsmöglichkeiten (vgl. S. 173ff.).

10 Vgl. zur gottgleichen Machtposition meinen Artikel «La technologie blockchain et la promesse crypto-divine d'en finir avec les tiers», in: *Études Digitales*, 1, 2019, (im Erscheinen)

11 https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543, letzter Aufruf: 7. März 2019. Von einem anderen Fall berichten de Filippi/Wright, S. 156f: Hier wurde eine Drohne durch den Einsatz eines smart contract auf den Weg gebracht, „ohne dass es eines zentralen Mittlers bedurfte, der das Gerät kontrollierte. Einmal gestartet, konnte der Code, der die Drohne verwaltet, nicht mehr gestoppt werden. Wenn der *smart contract* die Drohne in ein Gebäude oder in Richtung einer Person steuern würde, gäbe es für niemanden die Möglichkeit, seine Richtung zu ändern oder den Flug zu stoppen, ohne die Drohne komplett zu zerstören oder die Blockchain zu modifizieren."

12 Generell ist zu unterscheiden zwischen drei verschiedenen Blockchainkategorien. Neben der hier im Wesentlichen besprochenen „öffentlichen" Blockchain, gibt es private oder hybride Blockchains, die von einem zentralen Organ bzw. von einer Gemeinschaft an Unternehmen reguliert werden, die den Zugriff und den Nutzen für bestimmte Personen autorisieren. Vgl. dazu Claire Fénéron Plisson, «La blockchain, un bouleversement économique, juridique, voire sociétal», *A.D.B.S., « I2D – Information, données & documents »*, vol. 54, no 3, 2017, S. 21. Die zunehmenden privaten Blockchains werden oft als Rückschlag für das eigentliche Dezentralisierungsbestreben der Blockchain und verzweifelter Versuch der Konzerngiganten, ihre Position des Dritten zu bewahren, angesehen. Vgl. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains, letzter Aufruf: 13. März 2019.