

Oliver Leistert

### Bitcoin und Blockchain

2015

<https://doi.org/10.25969/mediarep/1138>

Veröffentlichungsversion / published version  
Zeitschriftenartikel / journal article

#### Empfohlene Zitierung / Suggested Citation:

Leistert, Oliver: Bitcoin und Blockchain. In: *POP. Kultur und Kritik*, Jg. 4 (2015), Nr. 2, S. 80–85. DOI: <https://doi.org/10.25969/mediarep/1138>.

#### Erstmalig hier erschienen / Initial publication here:

<https://nbn-resolving.org/urn:nbn:de:hbz:6:3-pop-2015-16678>

#### Nutzungsbedingungen:

Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.

Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

#### Terms of use:

This document is made available under a Deposit License (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual, and limited right for using this document. This document is solely intended for your personal, non-commercial use. All copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute, or otherwise use the document in public.

By using this particular document, you accept the conditions of use stated above.

## BITCOIN UND BLOCKCHAIN

*Oliver Leistert*

80 **D**ie öffentliche Wahrnehmung der digitalen Kryptowährung Bitcoin beschränkt sich auf zwei Anwendungen. In Kombination mit dem Tor-Netzwerk, das die derzeit weitgehendste anonyme Internetnutzung erlaubt, hat Bitcoin erstens erfolgreich eine Lücke geschlossen: Beide Technologien zusammen gestatten Markttransaktionen, die ohne das Wissen um die Identität von Käufer und Verkäufer zustande kommen (Tor); trotz der Anonymität vertrauen die Marktteilnehmer den Transaktionen, weil sie auf kryptografische Weise erfolgen (Bitcoin). Dass diese Kombination auch zu illegalen Geschäften einlädt, ist nicht weiter verwunderlich. Bitcoin erfährt inzwischen auch und gerade als Bezahlmittel für Drogen, Waffen und sogar Auftragsmorde Aufmerksamkeit in der Tagespresse. Dass Bitcoin z.B. aber auch als simples Tool für Geldüberweisungen von migrantischen ArbeiterInnen in ihre Heimat benutzt wird, erlangt weniger Beachtung.

Die zweite Anwendung bringt ein Problem jeder Währung mit sich: Es wurde so heftig mit Bitcoin spekuliert, dass die Volatilität der Währung ihre Bezahlfunktionalität bedrohte. Eine Währung ohne zentrale Ausgabestelle, die Geldpolitik betreiben und damit Fluktuationen einer Währung bekämpfen kann, ist hierfür sehr anfällig. Seit einigen Monaten jedoch hat sich der Kurs für einen Bitcoin bei ca. 200 Euro eingependelt, deshalb ist Bitcoin zunehmend als Bezahlmittel gefragt. Viele Banken, Finanzdienste und Händler akzeptieren bereits Bitcoin (von Dell Computer bis zur »taz«) oder erarbeiten Strategien, wie mit dieser Erfindung umzugehen ist (PayPal steht besonders unter Druck).

Gleichzeitig sind einige Defizite der Kryptowährung bekannt geworden, die zeigen, wo die Grenzen von Bitcoin als Wahrung liegen: Transaktionen dauern in der Regel eine halbe bis zu einer Stunde. Das mag schnell erscheinen, aber im Vergleich zu zentralisierten Systemen kann es ein Nachteil sein. Auerdem ist die Menge an Bitcoins systemisch begrenzt. Bisher sind ca. 14.221.000 Bitcoins errechnet worden, insgesamt werden es 21 Millionen sein (dies ist ins Programm eingeschrieben). Da Bitcoins um mehrere Stellen dezimal geteilt werden konnen, stellt das aber keine eigentliche Wachstumshurde dar, wenn der Kurs nur hoch genug ist. Dennoch wird Bitcoin, so wie es derzeit implementiert ist, niemals substantielle Anteile an Wahrungstransaktionen im globalen Mastab meistern. Bitcoin skaliert nicht optimal.

Trotzdem besteht kein Zweifel, dass die Person oder die Personen, die sich hinter dem Pseudonym Satoshi verbergen und 2008 mit dem Ausrollen der Bitcoin-Infrastruktur begannen, begnadete Programmierer, Okonomen und Kryptologen sind. Ihnen ist es gelungen, zentrale Probleme, an denen Vorlauffer von digitalen Kryptowahrungen gescheitert waren, auf auerst elegante Weise zu losen – vor allem das Problem des ›Double Spending‹, das bisher nur zentrale Verifizierungsinstanzen wie Banken/Staat oder Dienstleister wie Western Union und PayPal losen konnten. Das obligatorische Kriterium einer Wahrung (zu gewahrleisten, dass ein Coin nicht zweimal uber den Tresen wandert und behauptet, zwei zu sein) erfullt Bitcoin mit Finesse.

Es ist genau diese Losung, die Bitcoin jenseits seiner Funktion als Wahrung interessant macht. Andere Betrachtungen – seien es die Diskussionen uber das Drogengeld oder die Fantasien von US-Rechtslibertaren a la Rand Paul, die in Bitcoin das Ende des tyrannischen Staates sehen, dessen Geldmonopol immer schon mit Argwohn betrachtet wurde und dessen Steuern illegitim seien – verstellen blo den Blick auf eine viel radikalere Erfindung, die es in sich hat und die bisher kaum diskutiert wurde: die Blockchain!

Bitcoins stellen, wenn die Perspektive nur um einige Grad gedreht ist, lediglich eine von vielen denkbaren Anwendungen dar, welche die Blockchain ermoglicht. Die Blockchain ist eine neue Form von Organisation – eine Organisationsform unabhangig von zentralen Instanzen, dezentral auf tausende Rechner verteilt (und damit praktisch nicht abschaltbar), von niemandem kontrollierbar oder beeinflussbar: wahrhaftig autonom. Und sie kann etwas, was in der verwalteten, kapitalistischen, marktformig organisierten Welt standig passiert: sie kann verifizieren. Die Blockchain von Bitcoin (und dem Modell folgend andere Blockchains, die inzwischen von diversen Start-Ups, z.B. von Ripple, ins Leben gerufen werden) ist eine von auen unbeeinflussbare, kryptografisch arbeitende Verifizierungsorganisation, mit der jede Datei (und was ist heute nicht irgendwann eine Datei!) verifiziert werden kann. Sie kann beweisen, dass es eine Datei gibt und seit wann es sie gibt. Die Blockchain ist ein autonomer Validator von Information; sie ist ein Registrierbuch von Transaktionen, das

vollkommen transparent ist, aber niemandem gehört. Die Blockchain muss den ‚Commons‘ zugesprochen werden. Sie ist ein Ledger, wie es auf Englisch heißt, den alle benutzen können. Die Blockchain ist ein verteiltes System, das auf kryptografisch erzeugtem Konsens aufgebaut ist, in dem Daten sicher aufbewahrt und verifiziert werden können. Ob es Bitcoins oder andere Daten sind, spielt keine Rolle.

Die Zeitschrift »Pop. Kultur und Kritik« analysiert und kommentiert die wichtigsten Tendenzen der aktuellen Popkultur in den Bereichen von Musik und Mode, Politik und Ökonomie, Internet und Fernsehen, Literatur und Kunst. Die Zeitschrift richtet sich sowohl an Wissenschaftler und Studenten als auch an Journalisten und alle Leser mit Interesse an der Pop- und Gegenwartskultur.

»Pop. Kultur und Kritik« erscheint in zwei Ausgaben pro Jahr (Frühling und Herbst) im transcript Verlag. Die Zeitschrift umfasst jeweils 180 Seiten, ca. 20 Artikel und ist reich illustriert.

»Pop. Kultur und Kritik« kann man über den Buchhandel oder auch direkt über den Verlag beziehen. Das Einzelheft kostet 16,80 Euro. Das Jahresabonnement (2 Hefte: März- und Septemerausgabe) kostet in Deutschland 30 Euro, international 40 Euro.

**LUCIFER**, Jackson Pollock, 1947 © Pollock-Krasner Foundation / VG Bild-Kunst, Bonn 2015

Ein Beispiel, wofür die Blockchain, ein gigantischer Wust an Zahlen, den tausende vernetzte Rechner verteilt mit sich führen, zu benutzen wäre, ist das Projekt »Proof of Existence« des argentinischen Programmierers Manuel Aráoz. »Proof of Existence« ist gewissermaßen der abstrakteste und einfachste, aber fundamentalste Einsatz der Blockchain: Auf dem Portal lässt sich eine Datei hochladen, um zu beglaubigen, dass sie jemand zu einem bestimmten Zeitpunkt besitzt oder darüber verfügt. Dabei wird weder der Inhalt der Datei noch die Identität der Person, die den Proof erzeugt, für Dritte ersichtlich. Das verteilte System der Rechner, die über die Blockchain wachen, validiert durch die Produktion von kryptografischen Hashes die hochgeladene Datei als existent.

Ein Krypto-Hash ist in der Mathematik eine Funktion zur eindeutigen Abbildung von Zahlenwerten, deren Umkehrung jedoch unmöglich ist. Der Hash einer Zahl allein kann die Zahl, von der er stammt, nicht erzeugen. Gleichzeitig ist jeder Hash eindeutig, d.h. er kann nur von dieser einen Zahl stammen. Der Hash (auch Digest genannt) einer Nachricht (bzw. einer Zahl, aber das ist irrelevant) ist stets nur gültig für unveränderte Zahlenwerte. Der praktische Nutzen ist vielfältig: Hashes verifizieren beliebige Zahlenwerte, zeigen also an, dass die Zahl zu einem bestimmten Zeitpunkt (die Blockchain prozessiert auch Time Stamps) existiert hat.

Ein Beispiel aus dem Projekt »Proof of Existence« soll dies veranschaulichen: Von einer Datei, die den Besitztitel zu einem Grundstück benennt, wird der kryptografische Hash erzeugt und in die Blockchain gespeichert. Es ist nun jederzeit belegbar, dass es diese Datei in exakt diesem Zustand gibt. Die Blockchain validiert die Existenz und garantiert einen exakten Zustand der Datei. Wenn sich der Besitztitel ändert, muss folglich erneut ein Hash, anhand der neuen Datei, erzeugt werden. Was Notariate, Ämter und Gerichte erfüllen, kann, solange die Kryptografie ungebrochen ist, von einem autonom arbeitenden verteilten System bewerkstelligt werden. Hier wird klar, was der disruptive Vektor der Blockchain ist: Im Szenario einer Verwaltung, die alle Fragen von Vertrauen an Zahlen verarbeitende Maschinen abgibt, können die Dinge selbst, bzw. die auf sie verweisenden Dokumente, maschinell validiert und damit in ihrer Existenz bestätigt werden. Maschinen beweisen Existenzen. Die klassische Figur des Verwaltungsbeamten, über den man sich wenigstens noch aufregen konnte, weil er stets als Scharnier zwischen Lebensvollzug und verwalteter Welt wahrgenommen werden musste, wird ersatzlos gestrichen.

Mit solch einer verteilten Infrastruktur zur Validierung fallen zentrale, beglaubigende Instanzen, die allein vom Vertrauen leben, das ihnen zugesprochen wird oder das sie durch ein Gewaltmonopol simulieren, weg und erscheinen fortan überflüssig und fehleranfällig. In fast jeder Verkaufssituation spielt dies eine Rolle. PayPal lebt davon, dass Menschen, die Handel betreiben, ohne sich jemals zu Gesicht zu bekommen, eine Instanz brauchen, die beide Parteien im Vollzug des Handels kontrolliert. Die Blockchain ersetzt solche Mittelsmänner durch Validierung mittels verteilter Mathematik.

Ein anderes Beispiel: Aus der alltäglichen Computernutzung sind die Probleme bekannt, die durch Zertifikate des X.509 Systems auftreten. Wer Online-Banking betreibt, muss eine »gesicherte Verbindung« vom Arbeitsrechner zum Server der Bank aufbauen, damit niemand die Transaktionen belauschen kann. Nur woher weiß der Arbeitsrechner, dass das Zertifikat, das der Bankserver anbietet, auch wirklich von der Bank ist und nicht von Dritten, die den Datenverkehr mitschneiden wollen? Die aus Sicht vieler Sicherheitsforscher schlechte aktuelle Lösung baut auf Zentralisierung und Hierarchisierung auf: Es gibt eine Instanz, die verifiziert, dass das Zertifikat korrekt ist und damit das Gegenüber

authentifiziert. Das Vertrauen in diese Instanz, sei es die deutsche Telekom oder der chinesische Geheimdienst, ist aber vor allem blind. Die Verifizierer selbst sind nicht, oder zumindest praktisch nicht, verifizierbar. Aus diesem Dilemma, das weit über Online-Banking hinausreicht, gibt es nur einen Ausweg: Die verifizierende Instanz ist selbst vollkommen transparent, verteilt, nicht von einer einzigen Partei beeinflussbar und somit operativ immer konsensual.

Das Projekt Namecoin, ein Fork von Bitcoin, setzt genau hier an. Im Kern geht es darum, das zentralistische, letztlich vom Department of Commerce der US-Regierung kontrollierte Domain-Name-System zu ersetzen. Namecoin würde nicht nur die Authentifizierung der Gegenstelle in Sachen Verschlüsselung übernehmen, sondern zusätzlich auch die Auflösung der Domain in eine IP-Adresse dezentralisieren und somit weniger anfällig für z.B. Fishing-Attacken, aber auch Zensur sein. Domains abzuschalten wäre dann kaum mehr möglich. Das Konzept, das bereits im Test wunderbar läuft, verlegt die Auflösung der Domainnamen in IP-Adressen in die Blockchain, die alle jederzeit bei sich auf dem Arbeitsrechner mitführen können. Das ›Adressbuch‹ des Internet wird somit dezentral und autonom von kryptografischen Prozessen auf tausenden Rechnern verwaltet.

84

Die Anwendung von Hashes zur Validierung von Zahlen ist nicht neu und ein Standardverfahren für viele kryptografische, aber auch generell Programmier-Anwendungen. Neu ist, dass die Hashes, die zur Validierung benutzt werden, transparent verteilt auf beliebig vielen Rechnern gespeichert sind. Dass es sich im besten Fall um Server handelt, die durchlaufen und eine stabile Netzwerkverbindung haben, stellt noch keine Professionalisierung dar. Schließlich sind die derzeit experimentell entstehenden Anwendungen der Blockchain Webapplikationen.

Die Blockchain als Validator von Information fordert nicht nur Staaten und große Unternehmen heraus, deren machtvolle Position sich u.a. dieser vermittelnden Tätigkeit verdankt, sondern auch die Frage, ob eine Gesellschaft, die sich wesentlich über den Markt organisiert, bereit ist, Kernfunktionen der Identifizierung an autonome Maschinen abzutreten. Wo die Fantasie einer nicht vollends verschwundenen Handlungsfähigkeit des Menschen bisher die technische Zurichtung der Welt nach mathematischen Modellen gewissermaßen dialektisch ergänzt hat, stellt nun die Blockchain die Systemfrage: Als autonomes, kryptografisch konsensual operierendes System der Ordnungsstiftung kann sie den Grundpfeiler neoliberaler Regime, den Wettbewerb, paradigmatisch stützen, weil mit ihr externe Fehlerquellen, wie Korruption oder asymmetrische Marktzugänge, unwahrscheinlicher werden.

Die Blockchain löst damit operational eine problematische Konstellation, die in der zeitgenössischen Chiffre des Unternehmens und des unternehmerischen Selbst stets den Wettbewerb bedroht, nämlich die Frage, wie mit möglichst geringen strukturellen Bestimmungen der Wettbewerb als Form und Feld

produziert werden kann. Die Blockchain ist so gesehen die in Software sedimentierte Grundannahme neoliberaler Vergesellschaftung. Die Blockchain, als neutraler Verifizierer von Transaktionen, ist ein Mittel zur dauerhaften und beinahe kostenlosen Herstellung der Bedingung von Wettbewerb und Marktgeschehen.

Es wäre ein Leichtes, in der Blockchain auch andere Potenziale zu erkennen. Die Operation der Validierung ist schließlich kein Alleinstellungsmerkmal zeitgenössischer Gesellschaften. Sie ist bedeutsam für jede Problematisierung von Identität, Differenz oder sogar Ähnlichkeit. Die vielen Softwareprojekte und Start-Ups, die sich von dieser Technologie inspirieren lassen, zeigen, dass es eine Verengung wäre, ausschließlich auf die Wettbewerbsfunktionalität zu verweisen. Gleichzeitig ist zu konstatieren, dass sich keines dieser Projekte explizit gegen Markt und Wettbewerb richtet. Dies liegt daran, dass mit der Blockchain die Frage des Vertrauens aufgeworfen wird. Wenn das Vertrauen in das Gelingen einer Transaktion nicht mehr vom Menschen abhängt, erscheint die Technologie dahinter folgerichtig als Freiheitsversprechen, als Lösung eines Problems, für das bisher schwerfällige Institutionen, Verwaltungen und Regularien aufgeboten wurden. Der Charme von 37 Gigabyte Daten gegenüber einer Infrastruktur aus Verwaltungen und Handelskammern, die den Wettbewerb herstellen sollen, hat gewiss auch subversiven Charakter. Die Auslagerung des Vertrauens aus den Menschen in die Maschinen ließe sich lesen als Eingeständnis der mangelhaften Tauglichkeit des Menschen – oder als elegante Lösung eines das System hemmenden Problems.

Rückblickend sieht es also fast so aus, als seien Bitcoins nur ein Anreiz gewesen, die Blockchain in die Welt zu bringen. Denn das, was als Bitcoin-Mining bekannt ist, also das Errechnen von Bitcoins, bedeutet nichts anderes, als Material zur kryptografischen Validierung zu produzieren. Da allein hierzu wohl niemand Rechenkraft und vor allem Elektrizität (es sind sehr rechenintensive Operationen) zur Verfügung stellen würde, hat Satoshi als Belohnung eben Bitcoins erfunden für alle, die sich an der Produktion der Validierungsinstanz (teilweise gewiss unwissend) beteiligen. Bitcoins sind so gesehen nur die Belohnung für die Herstellung der Bedingung: das Errechnen der Hashwerte, die zum Identitäts- und Existenznachweis beliebiger Zahlen/Bilder/Filme/Musik/Texte/Urkunden/Akten gebraucht werden. Es bleibt abzuwarten, wie sich die Applikationen, die auf Blockchains basieren, entwickeln. Zweifellos ist das Feld, das sie aufmischen, durch machtvolle und ressourcenreiche Akteure belegt. Sollte aber ein Unternehmen wie Google oder Apple auf den Zug aufspringen (beide entwickeln derzeit intensiv ihre je eigenen, natürlich zentralisierten mobilen Bezahlssysteme) oder Finanzdienstleister auf die Blockchain umschwenken, würde ein sowieso unter Druck stehendes Gefüge wie der Handel erste Verschiebungen und Transformationen durchmachen, die das Regulationsvermögen von Regierungen und Handelsorganisation stark angriffen. ◆