

# OPEN DATA VS CRYPTO-WELTEN: CHANCEN UND RISIKEN IN DEZENTRALEN NETZEN

Elisabeth Hödl

Chief Scientific Officer, Watchdogs – The Data Company  
Auersperggasse 12, A-8010 Graz,  
www.watchdogs.at; elisabeth.hoedl@watchdogs.at

**Schlagnote:** *Open Data, Anonymität, Bitcoin, Blockchain, Ethereum, FinTechs, Smart Contracts*

**Abstract:** *Wir erleben eine Zeit großer Umbrüche, die durch die globale Vernetzung von Computern hervorgerufen wird. Es gehört zu den schwierigsten Aufgaben, die daraus folgenden Entwicklungen für Recht und Gesellschaft zu begreifen. Im folgenden Beitrag soll ein Zitat den Ausgangspunkt für die Überlegung bilden, wie Computernetzwerke in Zukunft die Finanzwelt verändern könnten. Bill Gates hat bereits im Jahr 1994 die provokante Äußerung getätigt: «Banking is necessary, banks are not». Was aber steckt dahinter? Es soll versucht werden, dieses Zitat mit Blick auf die gesellschaftliche Entwicklung in den gegenwärtigen Netzwerken zu analysieren und eine Antwort auf diese Frage zu finden. Dies soll in sieben Schritten geschehen.*

## 1. Einleitung

Alles begann mit der Idee der Dezentralisierung, die sich auf die weltweite Vernetzung unterschiedlicher Rechner bezog. Dezentralisierung war in den frühen Tagen des Internet für die Netzwerk-Community das Sinnbild für Emanzipation und Freiheit. Dezentralisierung war zugleich das Konzept einer libertären Gesellschaft. Dem englischen Philosophen *Francis Bacon* wird das Diktum zugeschrieben «*Scientia potestas est*». Was aber ist Wissen im digitalen Zeitalter? In der Monopolisierung der Märkte zeigt sich heute unter diesem Blickwinkel die Autorität von Internetgiganten wie Google und Facebook. Durch die Zunahme des Datensammelns und des Profiling nahm das Wissen über Menschen, ihre Persönlichkeit und ihre Pläne zu, die personalisierte Produktwelt wird zum Mittelpunkt der Wirtschaft. Die heutige Macht des Wissens manifestiert sich sohin in hochdetaillierten Datenprofilen über Personen, die es erlauben, die intimsten Lebensbereiche von Menschen zu enthüllen. Das Internet ist zum Spinnennetz geworden.

Vor diesem Hintergrund stellt Anonymität ein Ausgleichsprogramm in den Netzwerken dar, das es ermöglichen kann, Autonomie in Bezug auf die eigenen Daten zurück zu gewinnen.<sup>1</sup> Will man also die politischen Prozesse in den Netzwerken verstehen, muss man diese Polarisierung begreifen. So gibt es auf der einen Seite eine massive Öffnung von Informationen und das bewusste Teilen von Informationen und auf der anderen Seite Strömungen, die darauf abzielen, die eigene Autonomie mit Hilfe der Anonymität zu verteidigen. Am deutlichsten zeigt sich dieser Prozess am Beispiel des Geldes. Wie sich diese Entwicklung vollziehen könnte, soll im Folgenden in sieben Schritten demonstriert werden. Das Wechselspiel von Offenheit und Anonymität zu regulieren und zugleich auf die wachsende Maschinenautorität in den Netzwerken zu reagieren, ist eine besondere Herausforderung für das Rechtssystem.

---

<sup>1</sup> WALLACE, KATHLEEN A., Online Anonymity, in: Himma/Tavani (Hrsg.), *The Handbook of Information and Computer Ethics*, New Jersey 2008, S. 156–189.

## 2. Schritt 1: Die Idee der Dezentralisierung

Der britische Ingenieur und Computerwissenschaftler *Tim Berners-Lee* hat im Jahr 1989 die Idee des World Wide Web entwickelt und dabei das Konzept eines «universell verknüpften Informationssystems» verfolgt, das den Anspruch erhob, für jede Art von Information oder Auskunft einen Platz bereit zu halten. Seine Schlüsselbegriffe waren «universell», «verknüpft» und «linked». Aus der Idee der Open Source-Software wurde der Gedanke, frei verfügbares Wissen mit der Allgemeinheit zu teilen. In Fortführung der Idee einer dezentralisierten Struktur stellten freie verfügbare Datensätze, also Open Data, eine wichtige Rolle dar. Sie wurden zum weltweiten Phänomen.

Diese Entwicklung wird durch die Open Knowledge-Bewegung vorangetrieben, die Formate und Normierungen festlegt, unter denen Open Data veröffentlicht werden sollen, um möglichst umfassend ausgetauscht und genutzt werden zu können.<sup>2</sup> Dem Prinzip nach geht es um Information-Sharing und um Transparenz. Die wichtigsten Ziele der Open Knowledge-Bewegung dürfen in der Dezentralisierung und der Demokratisierung gesehen werden. Dem Staat kommt die Rolle zu, durch Transparenz die Informationsfreiheit der Bürger zu sichern und dabei eine Vorreiterrolle einzunehmen. Open Data-Portale weltweit sind Zeichen dieser Demokratisierungsbestrebungen.

Die Enthüllungen des US-amerikanischen Whistleblowers *Edward Snowden* im Jahr 2013 und die damit verbundene NSA-Affäre veränderten die Perspektive vieler Menschen und ließen sie fragen: Um welche Offenheit geht es eigentlich? Insbesondere in den Gemeinschaften junger Computerspieler bildeten sich Gruppierungen heraus, die sagten: «Open Source und Dezentralisation ja, aber ohne den Staat!» Vertreter dieses Zugangs bezeichnen sich als Kryptoanarchisten,<sup>3</sup> die Anhänger eines praktizierten Anarchismus im Cyberspace sind, die unter Nutzung freier kryptographischer Software die anonyme Kommunikation und den anonymen Handel möglich machen wollen.

## 3. Schritt 2: TOR – das Tor zur Anonymität

Anonymität bedeutet «Namenlosigkeit» und ist mehr als das. Anonymität stellt die Unmöglichkeit dar, Merkmale mit anderen bekannten Merkmalen zu verknüpfen. Es kann Anonymität in Bezug auf eine Gruppe (Öffentlichkeit) geben, während die gleiche Person anderen Menschen (etwa der eigenen Familie) bekannt ist.<sup>4</sup> Anonymität bedeutet sohin nicht, dass überhaupt keine verbundenen Merkmale vorliegen, sondern dass im relevanten Kontext die Koordination dieser Merkmale durch andere unmöglich ist, etwa weil diese geschützt oder voneinander getrennt sind. Die Isolation des Merkmals von anderen Merkmalen macht demnach aus, was eine Person anonym macht.

Damit ist der Begriff der Anonymität von dem der bloßen Unbekanntheit zu unterscheiden.<sup>5</sup> Erst wenn eine Handlung von anderen registriert wird, wird es überhaupt erst möglich, von Anonymität zu sprechen. Leute, die im Netz anonym bleiben wollen, nutzen Anonymisierungsdienste. Eines der bekanntesten Beispiele ist

---

<sup>2</sup> Für den Europäischen Raum findet sich der Rechtsrahmen dazu in der Public Sector Information-Richtlinie zur Weiterverwendung von Daten des öffentlichen Sektors Richtlinie 2003/98/EG kurz: PSI-Richtlinie und den Informations-Weiterverwendungsgesetzen; im Bundesgesetz über die Weiterverwendung von Informationen öffentlicher Stellen wurde die PSI-RL auf Bundesebene umgesetzt (Informationsweitergabe-Gesetz), BGBl I Nr. 76/2015.

<sup>3</sup> Der Techniker und Autor politischer Texte TIMOTHY C. MAY verteilte im Jahr 1988 einen Text mit dem Titel: *The Crypto Anarchist Manifesto* auf einer Kryptographie-Konferenz in Santa Barbara. <http://www.activism.net/cypherpunk/crypto-anarchy.html>.

<sup>4</sup> Ein Beispiel dafür ist TED KACZYNSKI, ein US-amerikanischer Mathematiker, der seiner Familie viele Jahre bekannt war, ehe die Familie überhaupt den Verdacht hatte, dass er der Unabomber (*university and airline bomber*) sein könnte, der in den Jahren zwischen 1978 und 1995 über sechzehn Briefbomben an verschiedene Personen in den USA verschickt hatte.

<sup>5</sup> Anmk: Es kann einen unbekanntem Autor geben, der nicht mit dem anonymen Autor gleichgesetzt werden kann.

Tor, «The Onion Router», ein Netzwerk zur Anonymisierung von Verbindungsdaten.<sup>6</sup> Tor funktioniert nach folgendem Prinzip: Die Verbindung zwischen zwei Endpunkten läuft über mehrere Zwischenstationen und jede Station kennt nur die unmittelbar vorherige und die unmittelbar nachfolgende, sodass niemand Herkunft *und* Ziel eines Pakets kennt. Wie sich erahnen lässt, dauert das Surfen mit Tor dadurch zwar spürbar länger, doch wer mit Tor surft, verwischt Spuren. «Tor», häufig auch der «Zwiebel-Router» genannt, bedient sich dabei einer zwiebelförmigen Informationsstruktur. Die Information wird verschlüsselt über verschiedene Server geschickt und ist am Ende wieder im Klartext lesbar.

#### 4. Schritt 3: Satoshi Nakamoto - Der Finanzkrise folgen die Bitcoins

Satoshi Nakamoto war es schließlich, der die Idee der Anonymisierung des Datentransports im Internet im Jahr 2008 für die Finanzwelt neu adaptierte. Wer Satoshi wirklich ist, ist bis heute nicht bekannt. Es könnte eine Einzelperson oder eine Gruppe von Personen sein. Der Öffentlichkeit wurde unter diesem Namen jedenfalls das Konzept der Bitcoins vorgestellt.<sup>7</sup> Bitcoin wird meist als die erste Kryptowährung bezeichnet, doch erscheint es treffender von der ersten dezentralen digitalen Währung zu sprechen. Tatsache ist, dass Bitcoins kurz nach Beginn der Finanzkrise eingeführt wurden, was drauf hindeuten könnte, dass damit eine konkrete Strategie verfolgt werden sollte.<sup>8</sup> Die gängige Abkürzung für die Währungseinheit ist BTC. Die Währung funktioniert anonym. Wer die Bitcoin-Software auf seinem Rechner installiert hat, wird Teil des Peer-to-Peer(P2P)-Netzwerkes. Die Software ist quelloffen, jeder weiß, wie sie funktioniert und jeder kann den Quellcode lesen. Das Installieren der Bitcoin-Software dauert Stunden, da jeder Nutzer die komplette Geschichte aller je getätigten Bitcoin-Zahlungen speichert. Jeder Computer, der Bitcoin nutzt, unterhält somit ein allumfassendes, von allen einsehbares Kontobuch, das im Moment 45 Gigabytes groß ist<sup>9</sup> (Anm.: das Zahlen mit Bitcoin ist auch ohne Installieren der Software möglich<sup>10</sup>). In dem einsehbaren Kontobuch lässt sich sehen, auf welchem Nummernkonto welche Summen liegen. Handlungen werden sichtbar, die Verknüpfbarkeit der Merkmale für die Identifizierbarkeit von Personen fehlt aber.

Vereinfacht gesagt: Jemand hat 100 BTC. Geht 1 BTC an A, gehen zugleich 99 BTC an den ursprünglichen Besitzer der 100 BTC. Die 100 BTC werden aus den Daten gelöscht. Damit ist jede Transaktion für alle Teilnehmer des Netzwerks nachvollziehbar. Bitcoin stellt ein digitales Kassenbuch dar, ein Kontobuch, das auf allen teilnehmenden Rechnern gleichzeitig einsehbar ist und völlig dezentral funktioniert. Neue Überweisungen werden minutenweise verzeichnet und allen Rechnern weltweit zugespielt. So entsteht im Lauf der Zeit eine Kette von Beweisen, die man Blockchain nennt. Blockchain ist die Kette und die Bitcoin-Transaktionen werden wie Perlen aufgereiht. Will einer der Nutzer etwas hacken, gibt es Millionen Gegenbeweise in der Blockchain. Dem System nach handelt es sich um ein dezentrales Buchhaltungssystem. Seit dem 4. Januar 2016 ist es möglich, an der Stanford University «Bitcoin Engineering» zu studieren.<sup>11</sup> Das Fach begreift sich als Abwandlung des Studiengangs «Crypto Currencies, the Blockchain and Smart Contracts», wobei der Kurs nicht die finanziellen Aspekte von Kaufen und Verkaufen lehrt, sondern Bitcoins als Protokoll betrachtet.

<sup>6</sup> Tor geht auf das US Navel Research Laboratory zurück. Vgl. <https://www.torproject.org/about/overview>.

<sup>7</sup> <https://bitcoin.org/bitcoin>.

<sup>8</sup> Vgl. EBERWEIN, HELGO/GERÉD, ARPÁD, Bits & Coins – Herausforderungen für sichere Zahlungsdienste im 21. Jahrhundert, in: Schweighofer/Kummer/Hötzendorfer (Hrsg.) Kooperation, Tagungsband des 18. Internationalen Rechtsinformatik Symposiums, IRIS 2015, Wien 2015, S. 631–638.

<sup>9</sup> Die Anzahl der Bitcoins ist mit 21.000.000 Einheiten festgesetzt, statt zwei gibt es acht Dezimalstellen. Damit ist 0,00000001 BTC der kleinste derzeit mögliche Wert.

<sup>10</sup> Unternehmen bieten Bitcoin Wallets an, das sind digitale Geldbörsen, die eine einfache Nutzung für Kunden möglich machen. <http://bitcoin-einfach.de/wallet> (27. Januar 2016).

<sup>11</sup> <http://bitcoin.stanford.edu/>.

## 5. Schritt 4: Ethereum – die Blockchain für den Finanzmarkt

Diese Idee wurde auch von dem heute 21-jährigen in Kanada lebenden Russen Vitalik Buterin aufgegriffen, der die Blockchain-Technologie nicht nur für Finanztransaktionen, sondern auch für weitere gesellschaftliche Bereiche anwenden will.<sup>12</sup> Buterin hielt sich in der Netzgemeinschaft der World-of-Warcraft-Spieler<sup>13</sup> auf und hatte sich in frühen Jahren für Bitcoin interessiert. Er brach sein Studium ab und beschloss sein Konzept «Ethereum» zu nennen und in einem White Paper<sup>14</sup> zu veröffentlichen. Der Name Ethereum, hat etwas mit dem Begriff Äther zu tun und stellt die Vision einer perfekten Blockchain dar. In Folge sammelte Buterin mittels Crowdfunding Geld und stellte in vier Wochen 18 Millionen Dollar auf, indem er 60 Millionen Einheiten der zum Projekt gehörenden Cryptowährung «Ether» verkaufte. Er landete damit die bisher größte Crowdfunding-Aktion der Geschichte.

Das entscheidende Moment für eine neue Ökonomie ist für Buterin der Umstand, dass die Blockchain nicht nur für die Finanztransaktion allein, sondern für jede Art von Wert eingesetzt werden soll. Egal, ob es sich um Münzen, Autos, Häuser, Diamanten, Kunst oder Aktien handelt. Seine Idee ist ein dezentrales Verzeichnis für sämtliche Vermögenswerte, mit der sicheren Möglichkeit, diese Werte zu transferieren. Sollte es gelingen, die Idee technisch zu realisieren, steht ein Angriff auf jede Art von Bürokratie an: Grundbuch, Notare und Behörden. Buterin traf in Tel Aviv auf Software-Entwickler, die sich auf die Programmierung von selbstaushührenden Verträgen spezialisiert haben.<sup>15</sup> Es sind sogenannte «Smart Contracts», die ohne Rechtsabteilung auskommen, weil ihre Ausführung durch die Blockchain kontrolliert wird. Es soll eines Tages Firmen geben, die sich selbst gehören, die vollständig von Computerprogrammen geführt werden, die ihre Geschäfte auf Basis von *Smart Contracts* selbstaushührend in digitalen Vertragswerken tätigen. Wie ein Vertrag mit einer Tageszeitung, die lesbar wird, sobald die tägliche Zahlung eingetroffen ist. Oder eine komplexe Schuldverschreibung, mit der in der Finanzbranche Kredite zerstückelt und weiterverkauft werden. Wie selbstfahrende Taxis, die auf die Maschinen an sich registriert sind und ihre Wartung durch Einnahmen finanzieren. Während Bitcoin auf finanzielle Transaktionen beschränkt ist, sollen bei Ethereum alle möglichen Transaktionen ausgeführt werden können. Sie müssen sich nur in Code übersetzen lassen. In Summe steht Ethereum für die Vision, den Kapitalismus an Maschinen abzugeben und die Wirtschaft komplett zu automatisieren.<sup>16</sup>

- Individuelle Währungen sollen geschaffen werden.
- Dienste aller Art sollen direkt angeboten werden (zum Beispiel Versicherungen).
- Finanzdienste, sollen angeboten werden und wie in einem Dorf, in dem die Kreditwürdigkeit vom Ruf einer Person abhängt, durch Micropayments skalierbar werden.

---

<sup>12</sup> GRASSEGGER, HANNES, Der digitale Lenin der Blockchain, 21. Dez. 2015, Capital, <http://www.capital.de/dasmagazin/der-digitale-lenin-hinter-der-blockchain.html> (27. Januar 2016).

<sup>13</sup> World of Warcraft (WoW) ist ein Computerspiel des US-amerikanischen Spieleentwicklers Blizzard Entertainment und zählt zum Genre der MMORPGs, das insbesondere von der Vernetzung der Spieler in Echtzeit lebt.

<sup>14</sup> <https://github.com/ethereum/wiki/wiki/White-Paper>.

<sup>15</sup> NORTA, ALEX/MA, LIXIN/DUAN, YUCONG/RULL, ADDI/KÖLVART, MERIT/TAVETER, KULDAR, eContractual choreography-language properties towards cross-organizational business collaboration <http://www.jisajournal.com/content/6/1/8/>, SpringerOpen (27. Januar 2016).

<sup>16</sup> Diese Idee findet sich in einem Buch des US-amerikanischen Softwareentwicklers, Systemberaters und Schriftstellers DANIEL SUAREZ. Darknet ist die soziale Utopie, die mittels dezentraler Produktion und nachhaltiger Energieerzeugung eine Alternative zu einer sich dystopisch entwickelnden Welt darstellt. Dieser Roman folgt den Ideen der Cyberpunk-Traditionen in denen Gesellschaften dargestellt werden, die mit einem schwachen Nationalstaat und regierenden privaten Konzernen eine entscheidende Rolle spielen.

## 6. Schritt 5: «Crypto Valley» in der Schweiz

Für das Ethereum-Projekt stellte sich die Frage, welches Land als Standort für einen Firmensitz in Frage kommen kann. Dabei waren folgende Faktoren ausschlaggebend: Kompetenz in Finanztransaktionen, Rechtslage (die eine Realisierung anonymer Transaktionen erlaubte) und Vertrauen. Die Wahl fiel auf die Schweiz, in der sich bereits einige Bitcoin-Unternehmen angesiedelt hatten. Zwischenzeitlich definiert sich das Schweizerische Zug als «Crypto Valley». Buterin arbeitet jetzt in Zug mit seinem Team an der Idee eines neuen Finanzsystems, das Firmengebäude wird als «Holon 000» oder «Raumschiff Ethereum» bezeichnet.<sup>17</sup> Schließlich zeigte auch das mächtige Netzgremium W3C um *Tim Berners-Lee* Interesse an Ethereum, das in die globale Kommission für Zahlungssysteme aufgenommen werden sollte, in der Google, Apple und zahlreiche Großbanken vertreten sind. In London wurde ein Blockchain-Forschungslabor eingerichtet und Ethereum zum wichtigsten Finanz-Experiment ernannt.

Neun der größten Banken der Welt, Goldman Sachs, Barclays, JP Morgan, State Street Corporation, UBS, Royal Bank of Scotland, Credit Suisse, BBVA, Commonwealth Bank of Australia haben sich verbunden, um in der in New York agierenden FinTech-Firma R3<sup>18</sup> ein Netzwerk zu gründen, das Blockchain-Technologie nutzen will, inzwischen umfasst das Bündnis 42 Banken<sup>19</sup>. Die Bank of England bezeichnet Blockchain als die «key technological innovation».<sup>20</sup> Der Blockchain-Verbund, der die weltgrößten Banken vereint, hat ein Dilemma zu lösen: *Wenn die Banken beginnen, sich selbst durch die Blockchain zu ersetzen, lösen sie sich von innen heraus auf. Wenn sie die Blockchain aber nicht nutzen, werden sie von der neuen Konkurrenz überrollt.* Daher evaluieren die Banken, welche Geschäftsbereiche sich automatisieren lassen, um dadurch den entscheidenden Kostenvorsprung in der immer härter werdenden Welt des digitalen Wettbewerbs zu erzielen. Im Bereich der FinTech – den sogenannten Finanztechnologien – werden Blockchains zur Nummer eins.<sup>21</sup> Der Kerngedanke ist: Wenn Geld Macht ist und Politik die Organisation der Macht, dann regiert derjenige, der die Geldströme lenkt.

## 7. Schritt 6: Das Geldsystem braucht Vertrauen

Die Frage war nun, was das zentrale Kriterium für das Konzept des neu gedachten Finanzmarktes sein musste. Um sich dieser Frage anzunähern, muss man erklären, was als Schwäche des bisherigen Systems betrachtet wird. Das Internet beruht auf dem TCP/IP-Protokoll, das den Bedürfnissen der Computer in den 1970er-Jahren angepasst ist. Netzwerke können zusammengeschlossen werden, weil sie auf der Basis des gleichen Protokolls funktionieren – diese Rechnernetzwerke bilden das Inter-Net. Das Ziel war Offenheit. Der Nachteil des Protokolls, der bis in die heutige Zeit reicht, ist natürlich, dass der Geldtransfer im Internet unsicher ist.

Dieses Sicherheitsdefizit macht das Bankensystem teuer, weil Unsicherheit, also der damit verbundene Vertrauensmangel, kompensiert werden muss. Ein Kunde muss Unmengen an Informationen preisgeben, um zu beweisen, dass er wirklich derjenige ist, der er vorgibt zu sein. Er muss Kartennummer, Name, Adresse, Alter

<sup>17</sup> GRASSEGGER, HANNES, Der digitale Lenin der Blockchain, 21. Dezember 2015, Capital, <http://www.capital.de/dasmagazin/der-digitale-lenin-hinter-der-blockchain.html> (27. Januar 2016).

<sup>18</sup> <http://r3cev.com/>.

<sup>19</sup> Williams-Grat, Oscar, A banking dream team is looking at technology that could «impact financial Services the way the Internet changed media», <http://www.businessinsider.de/blockchain-r3-membership-hits-42-as-it-looks-to-non-banks-2015-12?r=UK&IR=T> (27. Januar 2016).

<sup>20</sup> Nine of World's Biggest Banks Form To Join Blockchain Partnership, <http://www.reuters.com/article/us-banks-blockchain-idUSKCN0RF24M20150915> (27. Januar 2016).

<sup>21</sup> The great chain of being sure about things, in: The Economist, October 31st 2015, S. 21–24; The trust machine, The technology behind bitcoins could transform how the economy works, in: The Economist October 31st 2015, S. 11. Vgl. SCHULZ, BETTINA, Das ärgert Betrüger, Weniger Verbergen, weniger Kosten, wenige Arbeit: Die Technologie hinter Bitcoin könnte die Finanzwelt von Grund auf ändern – und sogar den Handel mit Diamanten oder Kunst, in: Die Zeit, 14. Januar 2016, S. 24.

angeben, also Daten, die beim Bargeldzahlen eigentlich nicht benötigt werden. Darin liegt der Schwachpunkt des Online-Finanzsystems. Man gibt Informationen privater Natur preis, damit das Vertrauen steigt und wird dadurch dem unsicheren Netz ausgesetzt. Mittelsmänner, die diese Transaktionen sicher machen, kosten Geld. Diese Kosten tragen die Bank oder das Kreditkarteninstitut als Zwischenstelle zur elektronischen Kundenüberprüfung oder eigene Banktypen, die dazu eingerichtet wurden, autorisierte Zahlungen zu vollstrecken. Die Institutionen stehen mit ihrem Namen dafür ein, den Datentransfer sicher zu gestalten, sie benötigen Sicherungscodes und Verifizierungen, um sich wiederum selbst abzusichern. Bis eine Zahlung dann tatsächlich abgeschlossen ist, vergeht Zeit in der die Mittelsmänner haften und es entstehen Kosten. Die Leistung der Finanzintermediäre heißt Vertrauen und eines der größten Probleme in diesem Zusammenhang ist die Verzögerung.

Bitcoin hat der Idee nach gezeigt, dass Zahlungen ohne Mittelsmänner möglich sind. Die Überweisungen sind fast kostenlos, benötigt werden Empfängeradresse aus Zahlen und Buchstaben plus Absender. 30 Bitcoins von XY gehen an ZW am 22. November 2015 um 17.05 Uhr. In der Praxis funktioniert die Transaktion mittels Blockchain anonym wie die Überweisung von einem Nummernkonto auf ein anderes. Und das eint die Programmierer-Internationale bei der Idee für eine neue digitale Finanzepoche. Man will eine perfekte Blockchain schaffen, die einen unfehlbaren Austausch von Werten ermöglicht. Der Ökonom *Yanis Varoufakis*, Griechenlands ehemaliger Finanzminister glaubt zwar nicht, dass es jemals apolitisches Geld geben könnte, er geht aber davon aus, dass die Technologie der Blockchain für den Finanzmarkt sehr wichtig werden wird. Der Goldstandard sei immer wieder zusammen gebrochen, weil unklar gewesen sei, welches Land wie viel Gold hat. Die Stärke der Blockchain-Technologie liege seines Erachtens in der Überprüfbarkeit der Werte.<sup>22</sup>

## 8. Schritt 7: Implikationen für Staat und Recht

Geht man davon aus, dass sich die technischen Probleme lösen lassen, die mit einer dezentralen Plattform wie Ethereum verbunden sind (etwa Stromkosten und Rechengeschwindigkeit)<sup>23</sup>, stellen sich für das Recht große Herausforderungen. Eine Gefahr anonymisierter Prozessen könnte etwa darin liegen, dass sie geeignet sind, staatliche Autorität zu untergraben. Eine naheliegende Frage ist beispielsweise, ob digitale dezentrale Krypto-Plattformen die Steuerflucht erleichtern und auf lange Sicht, die Finanzierung von Staaten nachhaltig gefährden können. Diese Befürchtung scheint insofern berechtigt, als das Untergraben staatlicher Autorität zum erklärten Ziel von Kryptoanarchisten und jener libertär denkenden Investoren ist, die sich bei der Entwicklung der Blockchain-Technologie im Finanzbereich beteiligen. Der US-amerikanische Investor *Peter Thiel*, unterstützt Ethereum finanziell<sup>24</sup> und auch den US-Politiker *Ron Paul*, der sich als Vertreter der Österreichischen Schule betrachtet, die in den USA in der Tradition einer libertären politischen Philosophie steht, die freie Märkte befürwortet. Die Kontrollbefugnisse der Staaten werden zunehmend beschränkt. Eine Gefahr der hier beschriebenen Anonymisierung und Dezentralisierung könnte sohin auch darin liegen, die staatliche Autorität zu untergraben und im Fall des Steuerrechts die Finanzierung von Staaten nachhaltig zu gefährden. Als Folge der Technisierung wird die Entgrenzung des Rechts evident.

Wie sich in diesem Beitrag gezeigt hat, werden Open Source-Projekte immer wichtiger. Die Frage ist allerdings, wohin die Entwicklung geht. Die Open Data-Bewegung, wie sie von *Tim Berners-Lee* verfolgt wurde,

<sup>22</sup> Yanis Varoufakis: «Österreich könnte den Euro verlassen» [http://diepresse.com/home/wirtschaft/international/4894300/Yanis-Varoufakis\\_Osterreich-konnte-den-Euro-verlassen?direct=4897530&\\_vl\\_backlink=/home/wirtschaft/international/index.do&selChannel=573](http://diepresse.com/home/wirtschaft/international/4894300/Yanis-Varoufakis_Osterreich-konnte-den-Euro-verlassen?direct=4897530&_vl_backlink=/home/wirtschaft/international/index.do&selChannel=573) (27. Januar 2016).

<sup>23</sup> Ethereum, Die Internet-Revolution stottert, <http://www.golem.de/news/ethereum-die-internet-revolution-stottert-1510-116821.html> (27. Januar 2016).

<sup>24</sup> RIZZO, PETE, \$100k Peter Thiel Fellowship Awarded to Ethereum's Vitalik Buterin, <http://www.coindesk.com/peter-thiel-fellowship-ethereum-vitalik-buterin/> (27. Januar 2016).

steht für Transparenz und Vertrauen in den Staat. Open Government geht vom mündigen Bürger aus, dem ein Recht auf Information zukommt<sup>25</sup>. Die anonyme Gemeinschaft löst Verantwortlichkeiten der Einzelnen auf.<sup>26</sup> Unter diesem Blickwinkel erlangt *Adam Smiths* «unsichtbare Hand des Marktes» eine neue Facette. Zugleich hat die globale Weltökonomie auch eine Tendenz zur Regionalisierung hervorgebracht. Immer mehr Politikfelder werden auf supranationaler Ebene und international auch von privaten und weniger legitimierten Organen bestimmt. Für die Staaten steigt damit die Bedeutung der Internet Governance und der Einsatz von Soft Law. Viele rechtliche Regeln der Cryptowelten werden sich zunehmend in der Hand der Technik finden, wie die Smart Contracts zeigen, die beim Aufbau des Ethereum-Projekts eine wichtige Rolle spielen. Die Automatisierung juristischer Verfahren wird jedoch nur dann im Sinne eines uns vertrauten Demokratieverständnisses funktionieren, wenn demokratisch legitimierte Institutionen als verantwortliche Entscheidungsträger bestehen bleiben. In der Arena der Netzwerke «Open Data vs Kryptowelten» ist daher genau zu unterscheiden, welcher Art von Macht wir uns unterordnen wollen, denn es sind Menschen, die an Visionen arbeiten, auch wenn Maschinen sie ausführen.

## 9. Glossar

**Bitcoin:** dezentrale, digitale Währung, die seit 2008 bekannt ist.

**BTC:** gängige Abkürzung für die Währungseinheit Bitcoin in Anlehnung an die Dreibuchstaben-Codes der ISO 4217.

**Blockchain:** die Struktur der Datenbank hinter Bitcoin, wobei alle Transaktionen auf allen beteiligten Rechnern gespeichert sind, in Blocks zusammengefasst, die jeweils mit sämtlichen Transaktionen verkettet sind (Kette=chain).

**Crypto Valley:** Zug in der Schweiz wird zum Kompetenzzentrum für Bitcoins während Zürich der konservative Finanzplatz bleibt.

**Ethereum:** dezentrale Plattform, die nach der Blockchain-Technologie anonyme Transaktionen aller Art erlaubt, gegründet von dem Russen Vitalik Buterin.

**Ether:** die Kryptowährung innerhalb von Ethereum.

**FinTech:** ist ein Kofferwort das sich aus den Wörtern *financial services* und *technology* zusammensetzt, Finanztechnologie ist ein Sammelbegriff für moderne Technologie im Bereich der Finanzdienstleistungen.

**Holon 000:** Das Firmengebäude von Ethereum in der Schweiz.

**Kryptoanarchismus:** praktizierter Anarchismus im Cyberspace unter Nutzung freier kryptographischer Software, mit der anonyme Kommunikation und anonymer Handel möglich sind.

**Micropayment:** Zahlungsverfahren geringer Summen, die vor allem beim Kauf von digitalen Gütern anfallen, nach herrschender Meinung fallen unter Micropayment Beträge zwischen 0,01 und 5,00 Euro.

**Peer-to-Peer (P2P) Connection:** Rechner-Rechner-Verbindung als synonyme Bezeichnung für eine Kommunikation unter Gleichen.

**Smart Contracts:** Computerprotokolle, die Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrages technisch unterstützen.

**TOR:** Ein Netzwerk zur Anonymisierung von Verbindungsdaten.

## 10. Literatur

BÜTTNER, RICARDO, *Automatisierte Verhandlungen in Multi-Agenten-Systemen*, Springer Gabler, Berlin (2011).

EBERWEIN, HELGO/ARPÁD GERÉD, *Bits & Coins – Herausforderungen für sicher Zahlungsdienste im 21. Jahrhundert*, in: Schweighofer/Kummer/Hötzendorfer (Hrsg.) *Kooperation*, Tagungsband des 18. Internationalen Rechtsinformatik Symposiums, IRIS 2015, books@ocg.at, Wien (2015), S. 631–638.

GRASSEGER, HANNES, *Der digitale Lenin der Blockchain*, 21. Dezember 2015, Capital, <http://www.capital.de/dasmagazin/der-digitale-lenin-hinter-der-blockchain.html> (27. Januar 2016).

<sup>25</sup> HÖDL, ELISABETH/ROHRER, TANJA/ZECHNER, MARTIN, *Open Data und Open Innovation in Gemeinden*, Wien 2015.

<sup>26</sup> WIEGERLING, KLAUS, *Philosophie intelligenter Welten*, München 2011, S. 47.

- GRAY, CHRIS HABLES, *Cyborg Citizen. Politik in posthumanen Gesellschaften*, Turia+Kant, Wien (2001).
- HÖDL, ELISABETH, *Software-Agenten: Juristische Einordnung und rechtliche Praxis*, in: Jusletter IT 11. Dezember 2013.
- HÖDL, ELISABETH/ROHRER, TANJA/ZECHNER, MARTIN, *Open Data und Open Innovation in Gemeinden*, Manz Verlag, Wien (2015).
- HÖDL/ZECHNER, *Was die Technologische Singularität für die Medienlandschaft bedeutet*, in: Schweighofer/Kummer/Hötzendorfer (Hrsg.) *Kooperation*, Tagungsband des 18. Internationalen Rechtsinformatik Symposions, IRIS 2015, books@ocg.at, Wien (2015), 125–132.
- NORTA, ALEX/MA, LIXIN/DUAN, YUCONG/RULL, ADDI/KÖLVART, MERIT/TAVETER, KULDAR; *eContractual choreography-language properties towards cross-organizational business collaboration* <http://www.jisajournal.com/content/6/1/8/>, SpringerOpen (27. Januar 2016).
- MAY, TIMOTHY C., *The Crypto Anarchist Manifest*, <http://www.activism.net/cyberpunk/crypto-anarchy.html>.
- SCHULZ, BETTINA, *Das ärgert Betrüger, Weniger Verbergen, weniger Kosten, wenige Arbeit: Die Technologie hinter Bitcoin könnte die Finanzwelt von Grund auf ändern – und sogar den Handel mit Diamanten oder Kunst*, in: *Die Zeit*, 14. Januar 2016, S. 24.
- SCHWARZ, GEORG, *Die rechtsgeschäftliche «Vertretung» durch Softwareagenten: Zurechnung und Haftung*, in Schweighofer/Menzel/Kreuzbauer (Hrsg.), *Auf dem Weg zur e-Person: aktuelle Fragestellungen der Rechtsinformatik*, Nr. 3 der Reihe *Schriftenreihe Rechtsinformatik*, books@ocg.at, Wien (2001), S. 65–72.
- SUAREZ, DANIEL, *Darknet, 6.A.*, Rowohlt, Hamburg (2015).
- VETTER, MICHAEL, *Ein Multiagentensystem zur Verhandlungsautomatisierung in elektronischen Märkten*, Stuttgart (2006).
- WALLACE, KATHLEEN A, *Online Anonymity*, in: Himma/Tavani (Hrsg.), *The Handbook of Information and Computer Ethics*, Wiley, New Jersey (2008), S. 156–189.
- WIEGERLING, KLAUS, *Philosophie intelligenter Welten*, Wilhelm Fink Verlag, München (2011).
- ZITTRAIN, JONATHAN, *Ubiquitous Human Computing*, Oxford Legal Studies Research Paper No. 32/2008.