BLOCKCHAIN (STATT) INTERNET OF THINGS?

Rolf H. Weber

Rolf H. Weber Prof. Dr. iur, Rechtsanwalt, Universität Zürich, Rechtswissenschaftliche Fakultät
Rämistrasse 74/38, 8001 Zürich, CH
rolf.weber@rwi.uzh.ch; https://www.ius.uzh.ch/de/staff/professorships/alphabetical/weberr/person.html

Schlagworte: ***Governance, IoT-Ökosystem, Mensch-Maschine-Beziehungen, Property Rights Management Systems, Smart Contracts***

Abstract: *Das Internet of Things vernetzt Gegenstände durch Kleinstcomputer untereinander. Technisch laufen die Vorgänge auf einem dem traditionellen Internet nahestehenden Netz ab. Mit der Blockchain-Technologie steht nun eine alternative Infrastruktur zur Verfügung, die sich für die Abwicklung von Transaktionen einsetzen lässt. Ob diese Tatsache zu einem Paradigmenwechsel führt, ist noch offen, aber technologische Veränderungen werden sicher eintreten und neue rechtliche Herausforderungen (z.B. mit Bezug auf die Governance, faktische Eigentumspositionen, Kontrolle intelligenter Systeme) bedürfen einer Lösung.*

1. Einleitung

Ungeachtet der Tatsache, dass der britische Technologie-Pionier Kevin Asthon[1] schon im Jahre 1999 das Internet of Things als System umschrieb, das Objekte in der physischen Welt miteinander verbindet, vermochte diese Erscheinung zu Beginn des Jahrtausends in der sozialwissenschaftlichen Diskussion keine grosse Beachtung zu finden. Erst in den letzten zehn Jahren ist das Internet of Things (IoT), das auf der RFID-Technologie (Radio Frequency Identification Device) beruht und die Nachverfolgbarkeit des Weges von Objekten sicherzustellen bezweckt, um Verluste zu vermeiden, vermehrt zum Gesprächsstoff geworden.[2]

Das IoT vernetzt verschiedene Gegenstände durch Kleinstcomputer untereinander, um automatisierte Abläufe zu ermöglichen. Technisch müssen also die Objekte befähigt sein, Informationen über deren Zustand in der realen Welt an die virtuelle Welt zu kommunizieren. Ein solcher Vorgang kann nicht unabhängig von der zugrunde liegenden Infrastruktur ablaufen; mit neuen Technologien vermag durchaus auch ein Paradigmenwechsel stattzufinden.

Das IoT basiert auf einem Object Naming Service (ONS), der mit einem Electronic Product Code (EPC) kombiniert ist. Technologisch baut der ONS als besonderes Netzelement auf dem Domain Name System (DNS) des «traditionellen» Internet auf, zeichnet sich indessen durch einige Spezifikationen aus (z.B. Standardisierungsvorgaben).[3] Hingegen bleiben verschiedene Ähnlichkeiten erhalten; vor allem setzt der IoT-Kommunikationsaustausch das Vorhandensein zentraler Intermediäre voraus. Mit der Blockchain-Technologie (allgemeiner der Distributed Ledger Technology) steht nun eine alternative Infrastruktur zur Verfügung, die dezentral strukturiert ist.[4] Diese grundlegende Veränderung in der Infrastruktur beeinflusst auch das IoT-Ökosystem;[5] einzelnen Aspekten dieser technologischen Neuerung ist im vorliegenden Beitrag nachzugehen.

---

1 Erstmals hat wohl Mark Weiser das Konzept des IoT angesprochen: Mark Weiser, The Concept for 21st Century, Scientific American, September 1991, 94 ff. Als Urheber des IoT wird meist Kevin Asthon genannt: Kevin Ashton, That «Internet of Things» Thing, RFID Journal, 22. Juni 2009 (http://www.rfidjournal.com/articles/views?4986) (alle Websites zuletzt besucht am 9. Januar 2019).

2 Die erste umfassende Studie stammt von Weber/Weber (2010).

3 Weber/Weber, 6 ff.

4 Allgemein zur Blockchain-Technologie statt Vieler vgl. Mougayar, 1 ff.

5 De Filippi/Wright, 157.

2. IoT-Ökosystem

Nach Beendigung der Arbeit einer von der Europäischen Kommission eingesetzten Expertenkommission (2011–2013)[6] bemühte sich insbesondere die Alliance of Internet of Things Innovation (AIOTI)[7] um die Schaffung eines dynamischen IoT-Ökosystems mit einer «Roadmap» von Handlungsfeldern bis 2020 (gestützt auf zwölf im Oktober 2015 publizierte Berichte).[8] Auf der technischen Seite entwickelt das European Research Cluster on the Internet of Things (IERC) eine Zusammenarbeits-Plattform für die Forschung.[9] Auch die International Telecommunications Union (ITU) ist im IoT-Bereich aktiv[10] und hat seit 2015 eine «Study-Group 20 – Internet of Things, smart cities and communities», die sich mit den Anforderungen an die Standardisierungen von IoT-Technologien befasst, eingerichtet.[11] Die amerikanische Federal Trade Commission (FTC)[12] ist mit Anhörungen von interessierten Kreisen in die Thematik eingestiegen; im Jahre 2017 hat sich die FTC dann mit einer Verlautbarung gemeldet[13] und auch einen IoT-Wettbewerb veranstaltet, bei welchem technische Lösungen und Werkzeuge zur «Bekämpfung» von Sicherheitsschwachstellen in IoT Geräten ausgezeichnet wurden.[14] Schliesslich ist die Dynamic Coalition on the Internet of Things (DC-IoT), die jeweils am Internet Governance Forum (IGF) ihre Erkenntnisse diskutiert (vorerst 2016 in Joao Pessoa und hernach vor allem 2018 in Paris[15]), daran, Leitlinien für «Global Good Practices» zu entwickeln.[16]

Rechtswissenschaftlich betrachtet sind in den IoT-Diskussionen während der letzten zehn Jahre als regulatorische Themen die Datensicherheit[17] und der Datenschutz[18] im Vordergrund gestanden. Dieses Risikopotential ist wegen der Vernetzung von Objekten und den ihnen zugrundeliegenden Daten auch offensichtlich. Zwischenzeitlich sind aber auch vermehrt vertragsrechtliche Aspekte[19] und insbesondere haftungsrechtliche Herausforderungen[20] in das Blickfeld geraten.

Demgegenüber steckt die Diskussion zur IoT-Governance weiterhin in den Kinderschuhen, selbst wenn durchaus anerkannt wird, dass sachgerechte Governance-Strukturen für den Erfolg des IoT wesentlich sind.[21] Insbesondere eine gewisse regulatorische Harmonisierung, die vermeidet, dass es zu Fragmentierungen in der technischen oder rechtlichen Interoperabilität der Systeme kommt, erscheint als geboten. Ein Vergleich der verschiedenen Regulierungsansätze lässt nach den bisherigen Erfahrungen den Schluss zu, dass der Top-Down-Ansatz (zumal im IoT-Kontext eine der ICANN vergleichbare Organisation fehlt) mit grösseren Problemen behaftet ist als das Bottom-Up-Modell; insbesondere bei den wichtigen Standardisierungen erscheint ein Aufbau

---

6 European Commission, Conclusions of the Internet of Things public consultation, https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation.

7 European Commission, The Alliance for Internet of Things Innovation (AIOTI), https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti; vgl. auch https://aioti.eu/.

8 European Commission, AIOTI Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2020, https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020.

9 IERC, Documents and Publications, http://www.internet-of-things-research.eu/documents.htm.

10 ITU, Overview of the Internet of Things: Next Generation Networks – Frameworks and functional architecture model, https://www.itu.int/rec/T-REC-Y.2060-201206-I.

11 Vgl. https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

12 FTC, Internet of Things, Privacy and Security in a Connected World, https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

13 FTC Offers Comment on Process Aimed at Improving Security of Internet of Things Devices, https//www.ftc.gov/news-events/press-releases/2017/06/ftc-offers-comment-process-aimed-improving-security-internet.

14 FTC, IoT Home Inspector Challenge, https//www.ftc.gov/iot-home-inspector-challenge.

15 Vgl. https://www.iot-dynamic-coalition.org/.

16 DC-IoT, Internet of Things Global Good Practices, https://www.iot-dynamic-coalition.org.

17 Weber/Studer, 715 ff.

18 Vgl. Weber, CLSR 2015, 618 ff. m.V. auf frühere Publikationen.

19 Vgl. Wendehorst, 367 ff.; Weber, Jusletter IT 2018, Rz. 3 ff.; Eggen, 1113 ff.

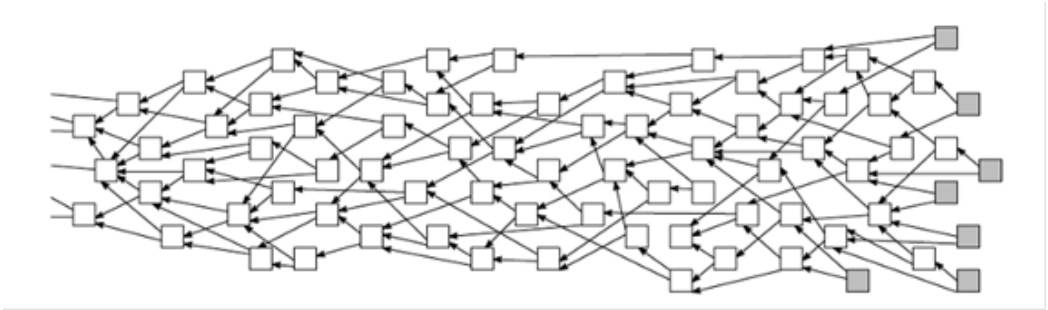
20 Vgl. Horner/Kaulartz, 506 ff; Weber, EuCML 2017, 207 ff.

21 Weber, Laws 2016, passim.

«von unten», der es erlaubt, mittels einer Multistakeholder-Teilnahme alle relevanten Stimmen einzufangen, als zukunftsweisend.[22] Dabei ist ein interdisziplinärer Ansatz, der datentechnikorientierte, wirtschaftliche und rechtssoziologische Elemente umfasst, zu verfolgen. Die anzustrebende Interoperabilität der angewendeten Standards wird bei Realisierung einer solchen langfristigen Governance am ehesten die erwünschte Finalität der Transaktionsausführungen erreichen können.[23]

3. Paradigmenwechsel durch die Blockchain-Technologie?

Heute drängt sich indessen die Frage auf, ob die sich derzeit entwickelnden Erscheinungsformen des IoT nicht durch neue Formen der Infrastruktur, insbesondere die Blockchain, «überholt» werden. Für die Blockchain (bzw. die sog. Distributed Ledgers) ist charakteristisch, dass sie auf einer dezentralisierten Infrastruktur beruhen, welche es den Teilnehmern ermöglicht, unwiderruflich Transaktionen abzuwickeln. Bildlich lässt sich die Ausgestaltung der Blockchain wie folgt darstellen:



Insbesondere entfällt auf der Blockchain die Notwendigkeit, mit einem zentralen Intermediär zu arbeiten, der die Informationen verteilt und ggf. bearbeitet. Abgesehen von Sicherheitsrisiken bei einer zentralen, eher angreifbaren Organisation erleichtert die dezentrale Infrastruktur die Abwicklung, weil beliebige Plattformen genutzt werden können.[24] Angesichts der Dezentralität der Infrastruktur ist zudem die Wahrscheinlichkeit kleiner, dass es zu Kapazitätsengpässen kommt.

Die Blockchain Technologie bietet auch die Grundlage für die Ausführung von Smart Contracts und damit für die Entwicklung neuer Geschäftsmodelle.[25] Ein Smart Contract ist ein Transaktionsprotokoll bzw. eine Computerroutine, die eine vernetzte selbstausführende Begründung von Vertragsbeziehungen bewirkt. Die Abwicklung erfolgt auf der Basis der strikt vorgegebenen (limitierten) transaktionalen Logik, d.h. auf der Basis des zur Durchführung vorbestimmten (determinierten) Code.[26]

Bei den heutigen IoT-Transaktionen entsteht ein vielgestaltiges Geflecht von Vertragsbeziehungen, die technisch über das Internet und damit über zentrale Intermediäre abgewickelt werden, ohne gesamthaft miteinander verknüpft zu sein. Bildlich lässt sich die Situation wie folgt darstellen:[27]

---

22 Weber, Laws 2016, 6, 8 f.

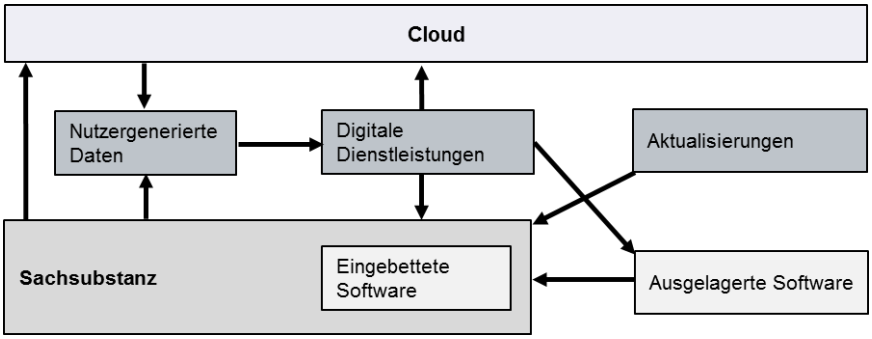
23 Zur Interoperabilität hinten Ziff. 4.2 und zur Finalität vgl. Blockchain Finality In The IoT, https://medium.com/coinmonks/blockchain-finality-in-iot-79e466406133.

24 De Filippi/Wright, 158.

25 Im Einzelnen dazu Weber, sic! 2018, 291 ff.

26 Kaulartz/Heckmann, 618 f.; Trüeb, 723 f.

27 Übernommen von Weber, Jusletter IT 2018, Rz. 13.



Bereits das IoT hat zwar, wie erwähnt, die Beziehungen zwischen den Personen und den Objekten, vermittelt durch technische Geräte oder Sensoren, verändert; mit den neuen Technologien, insbesondere der Blockchain, kommt es indessen zu einer ganz neuen Stufe der «Vermittlung», weil die Geräte und Sensoren durch autonome Software bestimmt sind.[28] «As the technology further matures, it is conceivable that one or more blockchains could power a next-generation Internet of Things, facilitating the emergence of new business models grounded on machine-to-machine transactions».[29] Aus diesen Gründen stellt sich die Frage, ob die Zukunft nicht eher bei einer nachfolgend noch genauer zu analysierenden «Blockchain of Things» liegt.

4. Herausforderungen für die Rechtsordnung

Der erwähnte mögliche Paradigmenwechsel durch die Blockchain-Technologie führt zu verschiedenen rechtlichen Herausforderungen, die künftig zu bewältigen sind bzw. die sich, im Vergleich zu den auf das IoT bezogenen Diskussionen, in verstärktem Ausmasse stellen; im Vordergrund stehen vor allem folgende Aspekte:

4.1. Verstärkung der Governance

Die Governance der Blockchain of Things, insbesondere auch im Falle des Einsatzes von Smart Contracts, ist erst noch sachgerecht zu entwickeln. Sinnvolle Anknüpfungspunkte leisten insoweit die Diskussionen zur Internet Governance; insbesondere der Multistakeholder-Ansatz erscheint als zukunftsweisend.[30] Weil sich internationale Vereinbarungen und einzelstaatliche Gesetzgebungen in globalen Netzwerken nur beschränkt durchzusetzen vermögen, sind alternative Regelbildungen unausweichlich. Die vom World Summit on the Information Society im November 2005 verabschiedete Definition des Multistakeholder-Ansatzes als «development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and the use of the Internet»[31] lässt sich ebenfalls auf die Governance in anderen technologisch geprägten Bereichen übertragen. Insbesondere die Zivilgesellschaft (aber auch die Akademie und die Unternehmen) sind am Prozess des Auffindens und Implementierens von Regeln im Blockchain-Ökosystem angemessen zu beteiligen.

Weil die Governance beim IoT schon bisher nicht sehr weit entwickelt ist,[32] bedarf es erheblicher zusätzlicher Anstrengungen, um stabile und vertrauenswürdige Strukturen auch auf der Blockchain bzw. auf den darauf entwickelten Plattformen zu verwirklichen. Verstärkt ins Blickfeld zu rücken ist zudem die Governance der Objekte bzw. Geräte («Device Governance»). Der Grund für eine solche Governance liegt darin, dass die Blockchain-Technologie als zugrunde liegende Anwendungs-Infrastruktur für die Objekte bzw. Geräte,

28 Sosnitza, 765, spricht schon beim IoT von «Software-Agenten».
29 De Filippi/Wright, 158.
30 Im Einzelnen dazu Weber, Cyberspace Framework, 126 ff. m.w.V.
31 Tunis Agenda for the Information Society, WSIS-05//TUNIS/DOC/6(Rev.1)-E, 18. November 2005, No. 34.
32 Vgl. vorne Ziff. 2 am Ende.

welche die Transaktionen zwischen Menschen und/oder Organisationen ermöglichen, dient.[33] Im Falle der Verwendung von Smart Contracts lassen sich die Governance-Regeln im anwendbaren Code programmieren, etwa mit Blick auf mögliche Funktionen von Objekten oder deren Operationalisierungs-Bedingungen.

Eine den technologischen Bedürfnissen angepasste Governance ermöglicht auch neue Geschäftsmodelle: Sind Objekte in der Blockchain of Things verfügbar, muss der Berechtigte nicht zwingend Eigentümer sein; vielmehr reicht in vielen Situationen eine Miete aus, z.B. wenn das Interesse besteht, ein Auto, das mittels eines Smart Contract auf der Blockchain angeboten wird, zu benutzen.[34] Leichter möglich wäre auch ein Time-Sharing; zur Verfügung gestellte Objekte lassen sich für eine beschränkte Zeitdauer «abrufen». In diese Richtung geht die deutsche Gesellschaft Slock.It, die gestützt auf Ethereum-basierte Smart Contracts den Verbrauchern die Möglichkeit einräumt, gewisse Objekte (z.B. Fahrräder, Abstellräume, Wohnungen) zu mieten oder in anderer (ähnlicher) Weise zu nutzen.[35]

4.2. Rechtliche Interoperabilität

In den letzten Jahren hat der Begriff der rechtlichen Interoperabilität («legal interoperability») an Bedeutung gewonnen; inhaltlich geht es darum, dass normative Regeln grenzüberschreitend (d.h. in verschiedenen Jurisdiktionen) einen gewissen Grad an Einheitlichkeit aufweisen. Damit soll eine für Online-Geschäftsmodelle negative Fragmentierung von Märkten vermieden werden.[36] Die rechtliche Interoperabilität lässt sich in verschiedenem Ausmasse anstreben; am weitesten geht die volle Harmonisierung von Regeln, etwas weniger ambitiös ist eine grundsätzliche Standardisierung der Rahmenbedingungen, die auch von privaten Selbstregulierungs-Organisationen angestrebt werden kann, wenn der staatliche Gesetzgeber deswegen nicht bemüht werden soll.[37]

Die rechtliche Interoperabilität trägt dazu bei, dass Abläufe technologischer und wirtschaftlicher Natur besser voraussehbar sind. Kommen in verschiedenen Ländern ganz unterschiedliche rechtliche Vorgaben zur Anwendung, wird der grenzüberschreitende Verkehr stark erschwert bzw. unattraktiv gemacht.[38] Die von der Dynamic Coalition on the Internet of Things formulierten, von Partikularinteressen nicht beeinflussten «Global Good Practices» sind ein erster Schritt in diese Richtung.[39]

4.3. Property Rights Management Systems

Im Kontext der Immaterialgüterrechte, v.a. der Urheberrechte, entwickeln die Verwertungsgesellschaften schon seit 20 Jahren sog. Digital Rights Management Systems (DRMS), die den Rechteinhaber in die Lage versetzen sollen, technisch zu verhindern, dass Unberechtigte sich die Vorteile der Verwertung geschützter Rechte aneignen können. Mit diesem Vorgehen wird also die Technik eingesetzt, um ein wirtschaftliches Resultat zu erreichen, das gegebenenfalls durch das Gericht festgelegt wird, d.h. die DRMS ermöglichen eine private Rechtsdurchsetzung.[40] Wenn die Entwicklung in die Richtung einer Blockchain of Things geht, erweist es sich indessen als angebracht, vertieft über Property Rights Management Systems (PRMS) nachzudenken, die in der Lage sind, physische Geräte anzuleiten und zu überwachen.[41]

Diese allgemeine, von früheren Erfahrungen, die zeigen, dass Verbraucherrechte ggf. durch technische Schutzmassnahmen eingeschränkt werden könnten, geprägte Einschätzung beruht auf folgender Überlegung: Der

---

33 De Filippi/Wright, 160.
34 Vgl. auch Nie/Erbring, 14 ff.
35 Vgl. https://slock.it/.
36 Eingehender dazu Weber, Laws 2016, 5.
37 Vgl. dazu Weber, Cyberspace Framework, 22 ff.
38 Vgl. auch Palfrey/Gasser, 178 ff.
39 Vgl. vorne Ziff. 2 bei Fn. 16.
40 Für einen umfassenden rechtsvergleichenden Überblick vgl. Bechtold, 323 ff.
41 De Filippi/Wright, 162 ff. m.w.V.

eingesetzte Code (z.B. im Smart Contract) vermag technisch (auch) die rechtlichen Regeln zu bestimmen, welche den Gebrauch der Objekte bzw. Geräte sowie ebenso die Beschränkungen des Gebrauchs festlegen. Solche in freier Autonomie des «Anbieters» verordnete Vorgaben sind deterministisch, weil das Resultat schon im Voraus (durch die im Smart Contract programmierte Computerroutine) feststeht.[42] PRMS werden dadurch zu perfekten Durchsetzungssystemen, weshalb ihre Legitimität als private «Waffe» in der Rechtsordnung ausgewogen abgesichert sein muss.[43] «These systems can enforce rules by preempting any conduct that occurs outside of what is expressly permitted by the underlying code».[44]

Um Marktverzerrungen zu vermeiden, sind verschiedene normative Rahmenbedingungen mit Blick auf die Verwendung von PRMS einzuführen: (i) Regulatorisch ist sicherzustellen, dass die PRMS von den Anbietern (bzw. ihren Programmierern) nicht in einer Weise zum Einsatz gebracht werden, dass die Nutzer technische Beschränkungen hinsichtlich verbundener Objekte (Geräte) hinnehmen müssen oder ein Zwang zum Bezug anderer Objekte desselben Anbieters besteht. Für die Ausgestaltung dieses Pfeilers lässt sich auf die Erfahrungen im Wettbewerbsrecht zurückgreifen (sog. «Lock-in» Problematik»).[45] (ii) Personendaten «gehören» in erster Linie den davon betroffenen Individuen; aus diesem Grunde ist regulatorisch sicherzustellen, dass Anbieter von PRMS solche Daten nicht monopolisieren.[46] Die Schaffung dieser zwei wichtigen Pfeiler bedarf der weiteren rechtlichen Durchdringung mittels vertiefender Forschungsarbeiten.

4.4. Rechtsrahmen für intelligente Systeme

Auf der Blockchain laufen Transaktionen weitgehend ohne konkreten Personenbezug ab; zwar besteht Transparenz hinsichtlich der verwendeten Blöcke bzw. der Kette von Blöcken, nicht aber mit Bezug auf die hinter dem Private Key sich «versteckenden» Person. Für die in einer solchen Situation entstehenden Mensch-Maschine-Beziehungen, die auch im Kontext von IoT-Transaktionen eintreten können, sind neue Rechtsnormen zu entwickeln, die den «elektronischen Agenten» (bzw. die emanzipierten Geräte) ebenfalls zu erfassen vermögen.[47] Weil also typische menschliche Komponenten wegfallen (z.B. der bewusste Austausch von persönlichen Willenserklärungen), erweist es sich als notwendig, die Elemente des Konsenses und des «Aufbewahrens» von Transaktionen in angepasste Rechtsformen zu «giessen».[48]

Je mehr sich Objekte verselbständigen und gestützt auf künstliche Intelligenz in der Lage sind, «eigene» Entscheide zu fällen, umso stärker ergibt sich das Bedürfnis, die Rechte und Pflichten solcher intelligenter Systeme bzw. Roboter festzulegen.[49] Zusätzlich kann sich die Frage stellen, ob autonomen Systemen gegebenenfalls sogar die Rechtspersönlichkeit einzuräumen sei, mit der Folge, dass sie Träger von Rechten, aber auch Pflichten (mit potentiellen Folgen für die Haftungsordnung) wären.[50]

Im Lichte dieser Entwicklungen bemüht sich die Lehre um eine neue Kategorienbildung für Rechtsnormen, die für das Rechtsleben im Alltag wichtig sind und auch massgeblich von den interessierten Teilnehmern aus der Multistakeholder-Gemeinschaft geprägt werden. An die Stelle des mittelalterlichen *lex mercatoria* soll die *lex cryptographica* treten.[51] Angesprochen sind damit Selbstregulierungen der betroffenen Kreise, die sich aus den praktischen Bedürfnissen heraus entwickeln lassen, und zwar ähnlich wie architektonische (technologieoffene

---

42 Weber, sic! 2018, 291 f.

43 Zur Problematik des «perfect enforcement» eingehend Zittrain, 107 ff.

44 De Filippi/Wright, 163.

45 Vgl. Shapiro/Varian, 103 ff.

46 Vgl. auch De Filippi/Wright, 164.

47 De Filippi/Wright, 165.

48 Ein zusätzliches Thema, das sich vorliegend nicht vertiefen lässt, betrifft den Datenschutz; abgesehen vom bereits umfangreichen Schrifttum vgl. den im Rahmen des Europarates entstandenen Report on Artificial Intelligence (Konvention 108) vom 3. Dezember 2018, T-PD(2018)09Rev.

49 De Filippi/Wright, 165.

50 Zu dieser vorliegend nicht zu vertiefenden Frage statt Vieler vgl. Beck, 183 ff.

51 Vgl. Wright/De Filippi, passim, und erneut De Filippi/Wright, 168 f.

und zugleich den Code als mögliche Rechtsquelle anerkennende) Standards.[52] Inhaltlich geht es darum, eine Rahmenordnung zu schaffen, welche die rechtlich zwingend einzuhaltenden Grundpfeiler des Rechts verankert und Handlungsanweisungen für das Verhalten im Alltag gibt.

4.5. Haftungsordnung

Die Behandlung von technischen Geräten, die sich von den Menschen emanzipiert haben, ist einer genaueren rechtlichen Betrachtung zu unterziehen; neben den Vorteilen sind insbesondere die ethischen und rechtlichen (Haftungs-)Risiken genauer zu durchleuchten. Die traditionellen auftragsrechtlichen Regeln bedürfen einer regulatorischen Ergänzung, um zu verhindern, dass sich autonome «Befehle» verselbstständigen.[53] Auch die ausservertragliche Ordnung zur Verantwortlichkeit, die schwergewichtig auf den Deliktsnormen und den Bestimmungen zur Produkthaftung und zur Produktsicherheit besteht, vermag den neuen technologischen Gegebenheiten nicht mehr vollumfänglich gerecht zu werden und ist durch sinnvolle moderne Haftungskonzepte zu ergänzen.[54]

Abgesehen davon, dass der Sorgfaltsmassstab im Lichte der Automatisierung, wie sie für IoT-Transaktionen ungeachtet der verwendeten Infrastruktur eintreten dürfte, zu überdenken ist, erweist es sich als naheliegend, bei einer neuen Infrastruktur, wie sie die Blockchain-Technologie darstellt, stärker in Risikosphären und in Risikozuordnungsmodellen zu denken. Wer ein zur Verfügung gestelltes «Instrument» in Anspruch nimmt, trägt auch die Verantwortung dafür, dass kein Schaden verursacht wird. In automatisierten Systemen mit selbstlernenden Algorithmen sind die Abläufe so zu programmieren, dass identifizierte Risiken schnell entdeckt werden können und dass Verfahren implementiert werden, welche die Risiken minimieren. Zutreffend steht das Thema der Anpassung der Haftungsordnung auf der Tagesordnung der Europäischen Kommission.

5. Ausblick

Zusammenfassend lässt sich somit prognostizieren, dass die heutigen Erscheinungsformen des IoT zwar nicht völlig verschwinden, aber doch bis zu einem gewissen Ausmasse durch die Blockchain of Things abgelöst werden dürften. Die im Titel des Beitrages gestellte Frage lässt sich deshalb nicht mit einem klaren «Ja» beantworten, aber die Tendenz ist offensichtlich und die Quantität an IoT-Transaktionen auf der Blockchain wird steigen, weshalb es als gerechtfertigt erscheint, von einer Blockchain of Things zu sprechen.

Die neue dezentrale Infrastruktur verursacht indessen zusätzliche Herausforderungen, mit denen sich verschiedene wissenschaftliche Disziplinen (insbesondere die Ethik) auseinander zu setzen haben; das Recht ist dazu aufgerufen, angemessene Rahmenbedingungen zu formulieren, welche die oft fehlende menschliche Intervention zu kompensieren bzw. auszugleichen vermögen. Im Vordergrund stehen dabei die Aspekte der Governance und die Verhinderung der Ausübung von Machtpositionen kraft privater Durchsetzungssysteme. Digitale Rechtsbeziehungen, die sich zu automatisierten bzw. rein technologiebezogenen Abwicklungsmechanismen fortentwickeln, dürfen nicht aus dem regulatorischen Blickfeld entlassen werden.

---

52 Vgl. Dell'Erba, 48.

53 De Filippi/Wright, 167.

54 Eingehender dazu Weber, EuCML 2017, 207, 210; Horner/Kaulartz, 506 ff.

6. Literatur

Bechtold Stefan, Digital Rights Management in the United States and Europe, American Journal of Comparative Law 52 (2004) 323 ff.

Beck Susanne, Der rechtliche Status autonomer Maschinen, AJP 2017, 183 ff.

De Filippi Primavera/Wright Aaron, Blockchain and the Law, Cambridge Mass. 2018.

Dell'Erba Marco, Demystifying Technology. Do Smart contracts require a new legal framework?, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228445.

Eggen Mirjam, Home Smart Home. Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, AJP 2016, S. 1131 ff.

Horner Susanne/Kaulartz Markus, Rechtliche Herausforderungen durch Industrie 4.0: Brauchen wir ein neues Haftungsrecht?, in: Taeger (Hrsg.), Internet der Dinge, Edewecht 2015, 501 ff.

Kaulartz Markus/Heckmann Jörn, Smart Contracts – Anwendungen der Blockchain-Technologie, Computer & Recht 2016, S. 618 ff.

Mougayar William, The Business Blockchain, Hoboken/New Jersey 2016.

Nie Norman H./Erbring Lutz, Internet and Society, Stanford Institute for the Quantitative Study of Society 3 (2000), S. 14 ff.

Palfrey John/Gasser Urs, Interop: The Promise and Perils of Highly Interconnected Systems, New York 2012.

Shapiro Carl/Varian Hal R., Information Rules: A Strategic Guide to Network Economy, Cambridge Mass. 1999.

Sosnitza Olaf, Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht?, Computer & Recht 11 (2016), S. 764 ff.

Trüeb Hans Rudolf, Smart Contracts, in: Grolimund et al. (Hrsg.), Festschrift für Anton H. Schnyder, Zürich 2018, S. 723 ff.

Weber Rolf H., Realizing a New Global Cyberspace Framework, Zürich 2014 (zit. Cyberspace Framework).

Ders., Internet of Things: Privacy Issues Revisited, Computer Law & Security Review 31 (2015), S. 618 ff. (zit. CLSR 2015).

Ders., Governance of the Internet of Things – From Infancy to First Attempts of Implementation?, Laws, MDPI, Vol. 5(3), 2016, S. 1 ff. (zit. Laws 2016).

Ders., Liability in the Internet of Things, Journal of Consumer and Market Law 2017, S. 207 ff. (zit. EuCML 2017).

Ders., Smart Contracts: Vertrags- und verfügungsrechtlicher Regelungsbedarf?, sic! (2018), S. 291 ff. (zit. sic! 2018).

Ders., Internet of Things und Vertragsrecht, in: Jusletter IT Flash 7. Juni 2018 (zit. Jusletter IT 2018).

Weber Rolf H./Studer Evelyne, Cybersecurity in the Internet of Things, Computer Law & Security Review 32 (2016), S. 715 ff.

Weber Rolf H./Weber Romana, Internet of Things. Legal Perspectives, Zürich 2010.

Wendehorst Christiane, Besitz und Eigentum im Internet der Dinge in: Micklitz et al. (Hrsg.), Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, Baden-Baden 2017, S. 367 ff.

Wright Aaron/De Filippi Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographica, March 10, 2015, https://ssrn.com/abstract=2580664.

Zittrain Jonathan, The Future of the Internet and How to Stop It, London 2008.