Die Blockchain und das Recht. Das Recht der Blockchain?

Veio Zanolini

Von staatlichen Regelungen hin zur Blockchain-Governance?

I. Einleitung

Spätestens seitdem der Bitcoin im Dezember 2017 innerhalb weniger Wochen den Schlusskurs von USD 19'216.26 erreichte und ein Jahr danach auf USD 3'248.74 sank, stehen Kryptowährungen im Fokus der öffentlichen Debatte. Die Blockchain ist die Technologie hinter dem Bitcoin. Heutzutage dienen Blockchain-Anwendungen meist dazu, Vermögenswerte schnell und kostengünstig zu transferieren. Die neue Technologie ist allerdings nicht auf rein finanzielle Zwecksetzungen beschränkt. Aktuell bestehen Blockchain-Projekte sowohl im Bereich der öffentlichen Verwaltung als auch in allen wichtigen Branchen der Privatwirtschaft. In Estland soll es bei einer E-Heirat möglich sein, die Hochzeitsurkunde in einer Blockchain zu hinterlegen, was den Notar, das Standesamt und den Priester überflüssig macht.[1] Durch ein eigenes Netzwerk und ohne zentrale Datenbank und Autorität erlaubt die Blockchain-Technologie Transaktionen zwischen zwei Nutzern auszuführen und die entsprechenden Informationen digital, einmalig und fälschungssicher in einer öffentlichen Datenbank zu buchen. Damit ermöglicht eine Technologie erstmals die bisher fehlende Vertraulichkeit im Internet. Mit anderen Worten können zwei Nutzer im Netzwerk einer Blockchain eine Transaktion ausführen, ohne das Vertrauen infrage zu stellen und zu überprüfen.

Mit der steigenden Zahl der Befürworter digitaler Währungen und auf Blockchain basierter Anwendungen ist anzunehmen, dass auch der Anteil an Personengruppen zunimmt, die mit der neuen Technologie nicht wie erwünscht umgehen und diese für sich entdecken, namentlich Opportunisten, Spekulanten und Kriminelle. Die heutige soziale Umwelt ist stark durch Internet und Technologie bestimmt, die nicht nur Vorteile, sondern auch neue Risiken und kriminogene Faktoren mit sich bringen. Die individuelle Entscheidung zu solchen Verhaltensweisen dürfte von einer relativ komplexen Kosten-Nutzen-Analyse abhängen. Schliesslich bieten digitale Währungen grundsätzlich die Gelegenheit, Transaktionskosten zu minimieren und den Nutzen zu maximieren, nicht nur bei legalen, sondern auch bei deliktischen Handlungen. Hinzu kommt, dass das Risiko, entdeckt zu werden, durch die Anonymität in verteilten dezentralen Strukturen reduziert wird.[2] Das mit der Blockchain-Technologie verbundene

1 Vgl. Binder, Heiraten mit der Blockchain, abrufbar unter https://www.swisscom.ch/de/business/enterprise/themen/banking/ban-2017-001.html, [09.08.2019].

2 Durrant, Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations, CUNY Academic Works, New York 2018, 34 ff.

Missbrauchsrisiko muss rechtzeitig erkannt werden. Am Finanz und Wirtschaft Forum vom 30.03.2019 waren sich die Gesprächsteilnehmer darüber einig, dass allfällige Risiken, die sich in der neuen Technologie verbergen, so gut wie möglich kalkulierbar gemacht werden müssen. Denn man wisse ja nicht, was nach der Blockchain komme. Man solle dabei einen möglichst technologieneutralen Ansatz verfolgen. Mit einem pragmatischen Ansatz war auch die schweizerische Finanzmarktaufsicht (FINMA) einverstanden.[3] Somit stellt sich die Frage nach der Regulierung der Blockchain-Technologie, denn geeignete Massnahmen können getroffen werden, wenn die entsprechenden gesetzlichen Grundlagen vorhanden sind.

Nach einem kurzen Überblick über die Blockchain-Technologie und deren Anwendungen (II.) werden nachfolgend rechtliche Grundlagen und Richtlinien thematisiert (III.), die sich in der Schweiz spezifisch auf die Blockchain beziehen. Sodann werden konkrete Aspekte der gesetzlichen Regulierung der Blockchain diskutiert (IV.): Welche Herausforderungen stellen sich dabei angesichts der Natur und der Eigenschaften der neuen Technologie? Was soll die Regulierung überhaupt bezwecken? Worin bestehen Chancen und Risiken? Ferner wird auf die Programmierung der Blockchain fokussiert, deren Code in der Lage sein könnte, diverse Steuerungs- und Kontrollfunktionen zu übernehmen (V.). Durch diese Annäherungsweise an das vielfältige Thema werden die Chancen der Regulierung durch das Gesetz und die Technologie der Blockchain dargestellt. Aufgrund der gewonnenen Erkenntnisse werden schliesslich einige Hypothesen hinsichtlich einer neuen Governance in der Blockchain-Ökonomie diskutiert. Der Ausgangspunkt für den Begriff der Governance ist die theoretische Perspektive der IT-Governance, die auf drei Dimensionen gestützt ist: Entscheidungsrechte, Verantwortlichkeiten und Anreize.[4]

II. Zur Blockchain-Technologie und deren Anwendungen

In der Blockchain werden Transaktionen in einem digitalen Kontenbuch dokumentiert, dessen Daten auf von Freiwilligen in aller Welt zur Verfügung gestellten und vernetzten Rechnern verwaltet werden. Sodann wird das Kontenbuch mehrfach kopiert, wobei die Kopien untereinander prinzipiell gleichgestellt sind. Neu hinzuzufügende Transaktionen werden in allen Kopien des Kontenbuchs übernommen, nachdem es zu einer Übereinkunft[5] über den jeweils aktuellen Stand des Kontenbuchs gekommen ist. Die Sicherheit bei der Verwaltung des Kontobuchs wird durch den Einsatz der Kryptografie gewährleistet. Die Datenstruktur ist mit jener eines P2P-Netzwerks vergleichbar, es gibt keine zentrale Datenbank, die gehackt werden kann, allerdings ist das Kontenbuch öffentlich.

In struktureller Hinsicht besteht die Blockchain aus Blöcken, einer Kette («Chain») und dem Netzwerk. Während im Block die Informationen über die Transaktionen gespeichert sind, die über einen bestimmten Zeitraum in einem Kontobuch aufgezeichnet werden, verknüpft eine Kette die Blöcke mathematisch miteinander, dies anhand eines Hash-Wertes[6]. Jeder Block

3 Bösiger, Die Blockchain fordert neue Rechtsformen, Finanz & Wirtschaft Nr. 25 vom 30.03.2019.

4 Vgl. Beck/Müller-Bloch/King, Governance in the Blockchain Economy: A Framework and Research Agenda, Journal of the Association for Information Systems, 2018, Vol. 19: Heft 10, Beitrag 1., Ziff. 2.3, m.w.H.

5 Dazu näher Antonopoulos, Bitcoin & Blockchain, Grundlagen und Programmierung. 2. Aufl., Heidelberg 2018, 219 ff.

6 Der Begriff «Hash» stammt aus der Mathematik und bezeichnet eine kurze Zeichenfolge mit fester Länge und stellt die Abkürzung einer beliebig langen Zeichenfolge dar. Ein kryptografischer Hash-Wert wird in der Blockchain-Technologie als Prüfsumme oder Sicherungsmechanismus benutzt. Ändert sich ein Zeichen am ursprünglichen Inhalt des Datensatzes, so ändert sich der entsprechende Hash-Wert komplett. Der Hash-Wert dient also dazu, zwei Zeichenfolgen miteinander zu vergleichen und festzustellen, ob sie identisch sind. Auf der Blockchain wird derjenige Datensatz, der gespeichert werden soll, in einen Hash-Wert umgewandelt und dieser im Block gespeichert. Grundsätzlich ist alles in einen Hash-Wert umwandelbar, es kommt dabei weder auf die Art noch auf die Grösse des Datensatzes an (vgl. Gyr, Blockchain und Smart Contracts, Die vertragsrechtlichen Implikationen einer neuen Technologie, Bern 2019, S. ii). Das Besondere am Hash-Wert ist, dass dieser nicht ermöglicht, den ursprünglichen Wert zu rekonstruieren.

muss sich auf den vorherigen Block beziehen, ansonsten ist er ungültig. Anhand der Bitcoin-Blockchain zeigt sich, dass die Technologie nicht auf Komponenten wie Konten, Nutzern, Salden oder Zahlungen basiert, sondern auf niedriger Ebene angesiedelten kryptografischen Funktionen bzw. Primitiven. Diese zeichnen sich wie folgt aus: Kein Double-Spending, Unveränderlichkeit, Neutralität, sichere Zeitstempel, Autorisierung, Überprüfbarkeit, Buchhaltung, kein Verfallsdatum, Integrität, atomische Transaktionen, diskrete (unteilbare) Werteeinheiten, Beschlussfähigkeit, Zeitsperren/Alterung, Replikation, Fälschungssicherheit, Konsistenz, externe Zustände festhalten, vorhersehbare Emission.[7] Aus diesen Primitiven werden übergeordnete Konzepte bzw. Anwendungen abgeleitet.

Das Blockchain-Netzwerk ist sowohl verteilt als auch dezentralisiert. Verteilt ist es deshalb, weil seine Bestandteile auf mehreren Rechnern an unterschiedlichen Orten gespeichert sind. Die Dezentralisierung hängt hingegen davon ab, wie die Entscheidungsrechte verteilt sind.

Neben den Kryptowährungen stellen Token, Smart Contracts und Initial Coin Offering (ICO) wichtige Kategorien von Anwendungen der Blockchain-Technologie dar. Als blockchainbasierte Kryptowährung setzt sich der Bitcoin zusammen aus Benutzern mit eigenem Wallet, den im Netzwerk propagierten Transaktionen und den Miner, welche das verbindliche Kassenbuch für alle Transaktionen bzw. die Blockchain erzeugen.[8] Virtuelle Währungen gelten in der Schweiz als Vermögenswerte, jedoch nicht als Währung oder gesetzliches Zahlungsmittel.[9]

7 Diese Liste ist nicht vollständig; neue Grundbausteine kommen hinzu, wenn neue Funktionen eingeführt werden. Näheres dazu Antonopoulos (Fn. 5), 282 %

8 Blockchain.info [09.08.2019] stellt hingegen einen Blockchain-Explorer zur Verfügung.

9 Bundesrat der Schweizerischen Eidgenossenschaft, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, Bern 2018, 7 %

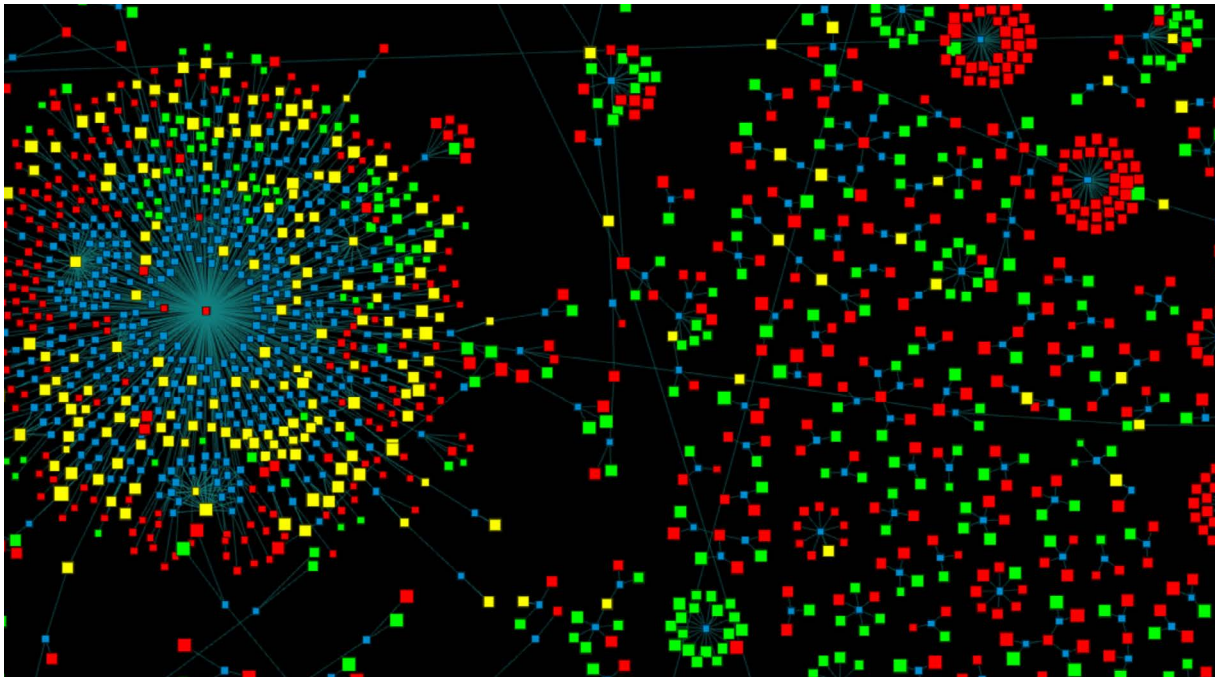

Abbildung 1: Visuelle Darstellung von Bitcoin-Transaktionen vom 20.08.2019 um 17.23.58 Uhr gemäss http://dailyblockchain.github.io.

Damit ein Datensatz (z.B. Wert oder Gegenstand in der realen Welt) Gegenstand von Transaktionen in einer Blockchain sein kann, braucht er einen eindeutigen Vertreter bzw. Token in der Blockchain. Für den Begriff «Token» besteht keine einheitliche Definition. Die FINMA qualifiziert Token aus einer finanzmarktrechtlichen Perspektive und teilt sie in drei Kategorien: Zahlungs-, Nutzungs- und Anlage-Token auf.[10] Je nach wirtschaftlicher Funktion repräsentiert ein solcher Token eine Aktie, Obligation oder ein Derivat. Ebenfalls in diese Kategorie fallen diejenigen Token, die physische Wertgegenstände auf der Blockchain handelbar machen.[11]

Was unter dem Begriff «Smart Contracts» zu verstehen ist, lässt sich nicht durch eine allgemeingültige Definition beschreiben. Smart Contracts können durch unterschiedliche Akteure zu unterschiedlichen Zwecken verwendet werden. Eine Vorreiterrolle kommt im Zusammenhang mit Smart Contracts der in der Schweiz ansässigen Ethereum-Stiftung zu, die diesen Begriff geprägt hat. Grundsätzlich handelt es sich um Codes auf der Blockchain, die mit anderen Smart Contracts interagieren, Entscheidungen treffen, Daten speichern und Ether – die Kryptowährung von Ethereum – versenden können. Die jeweiligen Eigenschaften können durch ihre Schöpfer bestimmt werden – die Ausführung und allfällige weitere Serviceleistungen werden jedoch durch die Ethereum-Blockchain vorgenommen.[12]

Schliesslich ist ein ICO eine Form öffentlicher Kapitalbeschaffung in digitaler Form für unternehmerische Zwecke. Die Anleger überweisen den ICO-Organisatoren finanzielle Mittel in Form von Kryptowährung und erhalten im Gegenzug blockchainbasierte Coins bzw. Token. Diese Token werden auf einer neu entwickelten Blockchain oder mittels Smart Contracts auf einer bereits bestehenden Blockchain geschaffen und verteilt gespeichert.[13]

Die Blockchain-Technologie hat viele Hürden zu überwinden, um zu einer Software zu werden, die zugleich eine Mainstreamlösung darstellt. Fraglich ist, ob die Technologie aktuell überhaupt flächendeckend einsetzbar wäre. In ihrer Anwendung ist sie komplex und schwer, man denke etwa nur an den enormen Energieverbrauch, der zum Durchführen der jeweiligen Algorithmen[14] erforderlich ist. Ferner dauert der Abrechnungsprozess im Bitcoin-Blockchain-Netzwerk immer noch rund zehn Minuten: schneller als im Rahmen herkömmlicher Zahlungssysteme, aber zu lange im Hinblick auf das Internet der Dinge. Wieweit ist das heutige Netzwerk skalierbar? Was passiert, wenn Tausende oder gar Millionen vernetzter Blockchains täglich Milliarden von Transaktionen verarbeiten? Die Antworten auf diese und ähnliche Fragen sind noch offen.

Hinzu kommt, dass die weltweite Infrastruktur nicht gleichmässig verteilt ist. Im Umgang mit der neuen Technologie ist festzustellen, dass diese für den Normalbürger ziemlich anspruchsvoll ist. Wer im Bitcoin-Netzwerk den privaten Schlüssel verliert, macht die darin enthaltenen Kryptowährungen unwiederbringlich, es sei denn, die Wallet-Firma hat sich dazu verpflichtet, den gegebenenfalls verlorenen Schlüssel wiederherzustellen. Jedenfalls fehlt ein zentralisiertes Institut wie eine Bank, die von vornherein bestimmte Dienste zur Verfügung stellt. Das Fehlen einer zentralen Autorität im Umgang mit Geld und Transaktionen verlangt im Allgemeinen eine erhebliche Verhaltensänderung, muss der Normalbürger doch nun allein und eigenverantwortlich sein Geld auf einem Stick speichern, seine Passwörter sichern und ein Backup dieser Daten an ver-

10 Eidgenössische Finanzmarktaufsicht FINMA (Hrsg.), Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Bern 2018.

11 Gyr (Fn. 6), xi ff.

12 Zu den Definitionsansätzen im Einzelnen Gyr (Fn. 6), 89 ff.

13 Gyr (Fn. 6), x.

14 Die wichtigsten Algorithmen sind aktuell Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Capacity, Proof of Burn (dazu näher developcoins.com, [09.08.2019]).

schiedenen Orten durchführen, damit sein Geld nicht plötzlich weg ist.[15]

III. Rechtliche Grundlagen

Die ersten praktischen Erfahrungen mit Kryptowährungen und Initial Coin Offerings haben zu den ersten Regulierungsversuchen geführt. Ein paar Beispiele: Bereits im Mai 2016 beschloss die Stadt Zug, dass Gebühren am Schalter der Einwohnerkontrolle bis zum Betrag von CHF 200.00 fortan in Bitcoin beglichen werden können. Dies war kein Zufall, hatten sich doch bereits einige Unternehmen aus dem Bereich der digitalisierten Finanzdienstleistungen und der Blockchain-Technologie im Kanton Zug angesiedelt. Im September 2017 ermöglichte das Handelsregisteramt dieses Kantons sodann die Gründung und Eintragung einer Aktiengesellschaft, deren Aktienkapital mittels Einlage der Kryptowährung Bitcoin als Sacheinlage liberiert wurde.[16] Nachdem 2017 in der Schweiz und in Liechtenstein die ersten Bankkonten für ICOs sowie für Projekte mit Kryptowährungen eröffnet wurden[17], hat die FINMA im Februar 2018 ihre eigenen Richtlinien erlassen. Es handelt sich um Prinzipien und Anforderungen, welche Gesuche um Eröffnung neuer Bankbeziehungen für Krypto-Projekte zu erfüllen haben. Im Zentrum der Richtlinien stehen Funktionalität und Übertragbarkeit von Zahlungs-, Nutzungs- und Anlage-Token, welche durch den ICO-Organisator ausgegeben werden. Da weder in der Schweiz noch international eine allgemein anerkannte Klassifizierung von Token besteht, spielt die Frage, ob diese bereits von Beginn des ICOs an handel- oder übertragbar sind, eine zentrale Rolle. Die Richtlinien der FINMA definieren ferner die Regeln zur Bekämpfung der Geldwäscherei.

Im Dezember 2018 hat der Bundesrat einen Bericht über die rechtlichen Grundlagen für *Distributed Ledger*-Technologie und Blockchain in der Schweiz erlassen.[18] Dieser bezieht sich in erster Linie auf die Anwendungen der Blockchain im Finanzsektor. Sodann werden Fragen im Zusammenhang mit dem Zivilrecht, dem Finanzmarktrecht und der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung behandelt. Die Frage lautet, wie die Blockchain in ihrer Natur und Anwendung *de lege lata* einzuordnen und zu beurteilen ist und ob die Rechtssicherheit mit Blick auf die neuen Entwicklungen durch neue, spezifische Normen sichergestellt werden soll. Ähnliche Fragen stellen sich, wenn man – statt der Blockchain – die Anwendungsmöglichkeiten virtueller Währungen unter die Lupe nimmt.[19] Das Fazit lautet, dass neue Regelungen schon deshalb erforderlich sind, weil sich die Blockchain oder die Kryptowährungen im geltenden Recht nicht vollständig einordnen lassen.[20]

In Bezug auf kryptobasierte Vermögenswerte stützt sich der Bericht des Bundesrates auf der von der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung durchgeführten Risikoanalyse. Diese kommt zum Schluss, dass weltweit ein Risiko des Missbrauchs kryptobasierter Vermögenswerte für Geldwäscherei und Terrorismusfinanzierung vorhanden ist. Jedoch unterstehen Personen und Institute, die mit solchen Vermögenswerten arbeiten und Finanzintermediation anbieten, bereits heute dem Geldwäschereigesetz. Bei Dienstleistungen, die keine Finanzintermediation darstellen – wie etwa bei Non-Custodial Wallet Anbietern –, sind Geldwäscherei oder Terrorismusfinanzierung unwahrscheinlich; in diesen Fällen besteht auch

15 Tapscott/Tapscott, Die Blockchain Revolution, Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert, 5. Aufl., Kulmbach 2018, S. 46, 323 ff. m.w.H.

16 Müller/Reutlinger/Kaiser, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, EuZ 2018, 80 ff., 84 f.

17 Petrovskaya, What makes Switzerland & Liechtenstein regulatory framework attractive to international blockchain, abrufbar unter https://innmind.com/articles/1836, [09.08.2019]).

18 Bundesrat (Fn. 9).

19 Dazu Müller/Reutlinger/Kaiser (Fn. 16), 80 ff.

20 Zum Problemfeld der Einordnung im geltenden Recht gehört auch das Verhältnis zwischen Landesrecht und EU-Recht. Sofern nun lediglich die EU und einige andere Länder neue Regelungen einführen, lässt sich eine Aktivität ohne Probleme in weniger intensiv regulierte Gebiete umgehen. Wünschenswert wäre daher ein global akzeptiertes Regulierungsrahmengerüst.

gemäss der Financial Action Task Force (FATF) kein Handlungsbedarf.[21]

Aufgrund dieser Übersicht ist festzustellen, dass hinsichtlich der Regulierung der Blockchain in der Schweiz Vorsicht und Pragmatismus herrschen.

IV. Regulierung der Blockchain durch das Gesetz[22]

In diesem Kapital wird die Regulierung durch Gesetze im formellen und materiellen Sinn der Blockchain-Technologie in Bezug auf deren Programmierung und Anwendung diskutiert. Die erste Ebene betrifft das Verhalten und die Aktivitäten der Endbenutzer. Einerseits könnten diese durch gesetzliche Regelungen direkt beeinflusst werden: Wer sich nicht an die gesetzlichen Pflichten hält, hat mit den gesetzlich statuierten Folgen zu rechnen. Andererseits könnten die Endbenutzer auch indirekt beeinflusst werden, etwa durch Steuern oder Verhaltensnormen, die über längere Zeit die geltenden Sozialnormen beeinflussen oder neue Sozialnormen schaffen. Will man hingegen die Aktivitäten der Endbenutzer direkt überwachen, so stellt die Verwendung von Pseudonymen sowie von Verschlüsselungstechniken und Datenschutzmassnahmen ein Hindernis dar, das durch den Einsatz von Data-Mining–Prozessen nur mit erheblichem Aufwand überwunden werden kann. In diesem Zusammenhang stellt sich grundsätzlich die Frage, ob die Regulierung auf der Ebene der Endbenutzer überhaupt sinnvoll ist, wenn ihnen mangels entsprechender Informationen das Unrechtsbewusstsein fehlt. Will man bei der Regulierung der Blockchain auf die Endbenutzer fokussieren, dann sollte dies in einer vernünftigen Art und Weise sowie in einem tragbaren Mass geschehen.

Eine weitere Ebene stellen die Internet Service Provider (ISP) dar. Wie sonst im Internet besteht ihre Aufgabe darin, dass sie durch das TCP/IP-Protokoll die Internetverbindung zur Verfügung stellen. Die ihnen zur Verfügung stehenden Protokolle enthalten zahlreiche und wertvolle Informationen über Verbindungen und Transaktionen innerhalb einer Blockchain sowie die Art und Weise, wie der Konsens zwischen der jeweiligen Rechnern («Nodes») zustande gekommen ist. Die Überwachung der ISP verspricht eine verhältnismässig gute Kontrolle über die Aktivitäten der Blockchains, denn sie sind nach wie vor in der Lage zu entscheiden, welche Rechner mit einer bestimmten Blockchain verbunden werden dürfen und welche nicht. Auf der Ebene eines ISP stellt sich das Verschlüsselungsproblem nur in einem beschränkten Umfang: Obwohl Verschlüsselungstechniken unter den Parteien, die eine blockchainbasierte Applikation verwenden, eingesetzt werden können, bleibt der Verkehr über das Netzwerk unverschlüsselt.

Neben ISP können natürlich auch die Suchmaschinen im Fokus staatlicher Regelungen stehen. So könnte z.B. die Indexierung von Webseiten so beschränkt werden, dass die Internet-Adresse bestimmter Anwendungen und relevante Hinweise unterbunden werden.

Gegenstand der Regulierung können ferner die blockchainspezifische Vermittler sein. Wenn die Blockchain-Technologie so konzipiert ist, dass in deren Netzwerk auf jegliche zentrale Datenbank und Autorität verzichtet werden kann, so schliesst dies das Auftreten neuer Vermittler nicht aus. Gemeint sind etwa neue Unternehmen, die Wallets zur Verfügung stellen, oder jene, die den Geldwechsel erlauben, entweder nur zwischen Kryptowährungen oder zwischen diesen und den herkömmlichen Währungen (Fiat-Währungen[23]). Sollen die Aktivitäten dieser Dienstleister überwacht werden, so besteht das Problem, dass diese ihren Sitz im In- aber auch im Ausland haben können. Somit würden sie zunächst einmal der

21 Bundesrat (Fn. 9), 149.

22 Gemäss dem Ansatz von De Filippi/Wright, Blockchain and the Law, The Rule of Code, Cambridge/London 2018, 173 ff.

23 Mit diesem Begriff werden heutzutage in erster Linie die Zentralbankwährungen gemeint. So fällt beispielsweise der Schweizer Franken genauso in den Bereich Fiat-Geld wie der Euro oder der US-Dollar.

Gesetzgebung des Staates ihres Sitzes unterstehen.

Dieses Problem gilt auch für die prominentesten Vermittler in einem Blockchain-Netzwerk: die Miner. Diese sind grundsätzlich in der Lage, zu eruieren, ob eine Transaktion technisch valide ist. Was die Transaktion hingegen bezweckt, können sie nicht interpretieren. Im Unterschied zu ISP sind sie nicht in der Lage, die Internetverbindungen durch eine tiefe Überprüfung deren Datenpakete zu überwachen. Für ihre Operationen profitieren die Miner nicht von einer Blockchain und stellen auch keine Blockchain zur Verfügung, sondern sind Bestandteil des Blockchain-Netzwerkes. Darin spielen sie eine autoritative Rolle, indem sie ultimativ entscheiden, ob eine neue Software, die Einfluss auf das grundlegende Protokoll einer Blockchain hat, überhaupt zugelassen wird. Dabei können sie die Angaben zum Verlauf von Transaktionen in einer geteilten Datenbank verändern oder neue Kontrollfunktionen im Netzwerk einbauen. Diese Möglichkeiten werden relevant, wenn eine Mehrheit der Miner in der Verwendung einer neuen Protokollregel übereinstimmen. Wie Miner-Pools entstehen können, zeigt sich anhand der Entwicklungen der grössten Blockchain-Netzwerke: Im Bitcoin-Netzwerk kontrollieren vier Miner-Pools über 50 % der gesamten Bitcoin-Blockchain; im Ethereum-Netzwerk sind es nur zwei. Würden diese Pools zusammenarbeiten, würden sie als eigentliche Herrschaftspools das gesamte Netzwerk kontrollieren.

Nun könnten die Miner und die Miner-Pools im Prinzip gesetzlich dazu verpflichtet werden, bestimmte, unerwünschte Aktivitäten im Netzwerk zu unterlassen oder zu verhindern. Würde sich eine Mehrheit von ihnen jedoch ausserhalb des gesetzlichen Anwendungsbereichs befinden, könnten sie jegliche Aufgaben und Funktionen übernehmen und im gesamten Netzwerk zur Verfügung zu stellen, ohne gesetzliche Folgen zu befürchten. Dieses Problem besteht bei dezentralisierten Netzwerken, in denen die Miner wichtige Entscheidungen selbständig treffen. Bei eher zentralisierten Blockchain-Netzwerken stellt sich das Regulierungsproblem grundsätzlich wie bei jedem anderen internationalen Netzwerk.

Ferner besteht die Möglichkeit, Normen zur Programmierung der Blockchain einzuführen, namentlich durch Vorgaben zur Herstellung des Codes der Blockchain. Denkbar wäre die Pflicht, im Blockchain-Netzwerk einen privilegierten Zugang für Behörden vorzusehen, der bei Bedarf die Ausschaltung bestimmter Funktionen erlauben würde. Auch hier würde sich das Problem des räumlichen Geltungsbereichs der jeweiligen Rechtsnormen stellen. Bei eher dezentralisierten Blockchain-Netzwerken würde sich insbesondere die Frage stellen, wie mit Miner umzugehen wäre, welche die Anwendung solcher Vorschriften verhindern würden.

Aufgrund der obigen Ausführungen kann der Eindruck entstehen, dass eine umfassende Regulierung der Blockchain eher unmöglich ist. Jedoch hat die Blockchain-Technologie mit internationalen verteilten Netzwerken – etwa P2P-Netzwerken – viel gemeinsam. Mit solchen Netzwerken leben wir schon seit zwei Jahrzehnten. Darüber wurde bereits vor der Finanzkrise von 2008 geforscht.[24] Die Regulierung der Blockchain-Technologie stellt daher kein neues Thema dar. Dabei empfehlen Quintais et al. (2019), es sei zu vermeiden, dass Technologie einerseits und Gesetze andererseits als zwei Welten dargestellt werden, als würden Letztere die Innovation und die Entwicklung der Blockchain von vornherein verhindern. Am Beispiel der Schweiz zeigt sich, dass die gesetzlichen Grundlagen und die Debatte über die Einführung neuer Regelungen die Vorbeugung von sozialschädlichen Risiken bezwecken. Rein präventive Regelungsbestrebungen, welche der Innovation und der Entwicklung der Blockchain-Technologie im Weg stehen würden, sind

24 Siehe etwa Goldsmith/Wu, Who Controls the Internet? Illusions of a Borderless World, Oxford 2006; Quintais et al., Blockchain and the Law: A Critical Evaluation, Amsterdam Law School Legal Studies Research Paper No. 2019-03, 19 f. m.w.H.

nicht ersichtlich. Das zeigen auch die Richtlinien der FINMA.

V. Der Code der Blockchain als Gesetz[25]

In einer Zeit digitaler Transformation setzt die Digitalisierung auf mehreren Ebenen eines Unternehmens – etwa der Produkte und Dienstleistungen, der Kanäle, des operativen Geschäfts (Arbeitsprozesse) und des Geschäftsmodells überhaupt – ihre Regeln durch und beeinflusst das menschliche Verhalten in mehrerer Hinsicht. Am besten ist die Digitalisierung im Gesamtkontext des jeweiligen Unternehmens zu betrachten. Somit stellt die Digitalisierung nicht nur ein Effizienzsteigerungsprogramm dar, sondern ist ein zentrales Element der Unternehmensstrategie, die zu einem Kulturwandel führt. Damit ist die Digitalisierung Chefsache und nicht bloss ein IT-Thema.[26] Bei der Digitalisierung von Produkten und Arbeitsprozessen werden Unternehmensstrategien in Codes umgesetzt: Kundenentscheidungen lösen Arbeitsprozesse aus und führen zu einem im Voraus festgelegten Ziel. Die Digitalisierung beschränkt sich nicht auf die Privatwirtschaft, sondern fasst auch in zahlreichen Tätigkeitsfeldern der öffentlichen Verwaltung Fuss.

Während die gesetzliche Regulierung der Blockchain – wie im vorherigen Kapitel dargestellt – zahlreiche Schwachstellen aufweist, könnte man davon ausgehen, dass die Technologie grundsätzlich in der Lage ist, ein deterministisches und selbstausführendes System zur Anwendung und Durchsetzung von Regeln zur Verfügung zu stellen. Wäre ein solches System wirksamer und effizienter als das Gesetz? Klar ist, dass die Technologie wenig Spielraum für Entscheidungen lässt, denn technische Prozesse werden meist durch klare und strenge Regeln gesteuert. In einem digitalisierten deterministischen System würde der Code zum obersten Gesetz. Mit den Worten von Charles Clark: «The answer to the machine is the machine»[27]. So könnten die Voraussetzungen zur Anwendung von Normen in blockchainbasierten Lösungen hartcodiert und automatisiert werden. Unter diesen Umständen würden die Unsicherheiten bei der Auslegung und Anwendung des Rechts erheblich reduziert oder gar eliminiert werden. Auch die Kontrolle über die Einhaltung der Gesetze für die Behörden wäre einfacher und effizienter. Durch den Einsatz einer Technologie, die nichts vergessen kann, würde die Gefahr von Manipulationen der Daten durch eine zentrale Stelle entfallen.[28]

Dabei stellt sich allerdings die grundlegende Frage, ob und wieweit sich Gesetze in technische Regeln und Codes übersetzen lassen. Das System einer Blockchain an sich ist eigentlich eine blinde Umgebung bestehend aus Codes; die Regeln werden vom Netzwerk unveränderbar interpretiert und ausgeführt. Die Absichten hinter dem Code werden jedoch nicht interpretiert.[29] Hingegen sind Gesetze in einer Sprache formuliert, die von Natur aus flexibel und zugleich mehrdeutig ist. Sie stellen einen Text dar, welcher einer Interpretation bedarf. Der Spielraum im Rahmen der Rechtsanwendung nimmt bei unbestimmten Rechtsbegriffen zu, deren Bedeutung nicht allgemein-abstrakt und von vornherein festgelegt werden kann, sondern erst im Kontext der Rechtsanwendung zu eruieren ist. Bei der Einbindung der Normen in ein Blockchain-Netzwerk droht somit sowohl ein Verlust als auch eine Umdeutung relevanter und unerlässlicher Norminhalte. Daher würden nur ganz bestimmte Normen mit eindeutigem (eher technischem) Inhalt in Betracht kommen.

Will man der Blockchain Steuerungsfunktionen und Kontrollaufgaben übertragen, würde die Anwendung von Gesetzen und sonstige Normen durch ein deterministisches System erfolgen, welches gemäss den obigen Ausführungen eine

25 Gemäss dem Ansatz von De Filippi/Wright (Fn. 22), 193 ff.

26 Bain & Company (Hrsg.), Von der Vision zur Transformation: Digitalisierung ist Chefsache, München/Zürich 2018.

27 Clark, The Answer to the Machine Is the Machine, in: Hugenholtz (Hrsg.), The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium, The Hague 1996.

28 Vgl. Abramowicz, Cryptocurrency-Based Law, Arizona Law Review 58/2016, 359 ff.

29 Gyr (Fn. 6), 212 ff.

höhere Effizienz versprechen würde. Dabei ist allerdings unklar, was unter einem solchen Effizienz-Konzept zu verstehen ist. Quintais et al. (2019) bringen ihre Skepsis zum Ausdruck: Wenn algorithmisch determinierte Entscheidungsprozesse dazu führen sollten, dass die ultimative Kontrolle und der Überblick des Menschen über diese entbehrlich werden und keine Möglichkeit mehr besteht, sowohl die Entscheidung selbst als auch das Vorgehen infrage zu stellen, dann sollte man eigentlich danach fragen, ob ein solches System überhaupt erwünscht, nicht bloss, ob dessen Realisierung technisch möglich sei.[30] Dieser Kritik ist zuzustimmen. Dass man in einer ersten Entwicklungsphase das Potenzial einer neuen Technologie genauer einschätzen will, kann verständlich sein. Trotzdem sollten die Bedürfnisse und die Interessen des Menschen und der Gesellschaft im Zentrum bleiben.

VI. Schlussfolgerungen

Mit dem Ausdruck «Blockchain-Technologie» werden verteilte und mehr oder weniger dezentral geführte Netzwerke bezeichnet. Die Blockchain-Technologie als solche, wie wir sie unter II. beschrieben haben, müsste allerdings nicht nur verteilt, sondern auch vollständig dezentral geführt werden. Denn alle Systeme, die ganz oder auch nur teilweise zentralisiert geführt werden, sind manipulierbar. Man muss also Blockchain-Systeme verwenden, die niemand, egal mit wie viel Computerpower er ausgestattet ist und mit wie vielen Computern er sich zusammenschliesst, verändern kann. Dass «Blockchain-Technologie» heutzutage als Sammelbegriff benutzt wird, ist deshalb verständlich, weil es das vollständig dezentralisierte System in der Realität bisher nur einmal gibt und das ist die Bitcoin-Blockchain. Wenn man von Blockchain-Netzwerken redet, heisst dies noch lange nicht, dass es dabei um vollständig dezentralisierte Netzwerke handelt. Vielmehr kommt es auf den Grad der Zentralisierung bzw. Dezentralisierung der Entscheidungsrechte an. Blockchain-Netzwerke, die nicht öffentlich zugänglich sind, werden im Allgemeinen einen höheren Grad an Zentralisierung aufweisen. Konkrete Beispiele sind Airbnb und Uber, hingegen folgt die Handelsplattform Swarm City in ihrer Organisationsstruktur einem dezentralisierten Ansatz.[31] Im Hinblick auf die Regulierung gilt: Je dezentralisierter die Netzwerke geführt werden, desto grösser ist die Herausforderung.

Gegenüber der mit dem Thema der Blockchain verbundenen Vielfalt überrascht kaum, dass eine umfassende Regulierung durch das Gesetz eher unmöglich erscheint. Wird einzig auf dezentral geführte Netzwerke fokussiert, so findet man Lösungsansätze zur Regulierung der Blockchain-Technologie nur im Kontext einer neuen Governance. Das Konzept der IT-Governance mit seinen Grundstrukturen ist in Bezug auf verteilte sowie dezentral geführte Netzwerke unbrauchbar.

Ob Smart Contracts zur Anwendung kommen oder nicht: Es ist aktuell nicht ersichtlich, wie Blockchain-Netzwerke in der Lage sein könnten, beliebige Gesetze zu ersetzen und autonom im Rahmen eines deterministischen, wirksamen und effizienten Systems zur Anwendung zu bringen. Selbst wenn der Anwendungsbereich der Smart Contracts auf Zertifikate und technische Regeln beschränkt sein wird, ist in vielen Branchen nicht nur mit neuen Arbeitsprozessen, sondern auch mit einer neuen Verteilung der Ressourcen zu rechnen.

Jede digitale Lösung wurde von Menschen erzeugt. Hoffentlich wird der Mensch künftig die Übersicht über die strategischen Entscheidungen behalten. Dass im Rahmen illegaler Aktivitäten Kryptowährungen als Zahlungsmittel benutzt wurden, konnte u.a. die Studie von Janze (2017) belegen. Die Ergebnisse dieser Untersuchung zeigen jedoch, dass das Fiat-Geld

30 Quintais et al. (Fn. 24), 19 % m.w.H.

31 Vgl. Beck/Müller-Bloch/King (Fn. 4), Ziff. 2.3, m.w.H., 16.

das gleiche Schicksal teilt.[32] Daher fehlen überhaupt Hinweise darauf, dass der Umgang mit Kryptowährungen mit einem erhöhten Kriminalitätsrisiko verbunden ist, wie oft vermutet wird.[33]

Während ein enger kausaler Zusammenhang zwischen Blockchain bzw. Kryptowährungen und kriminellen Verhaltensweisen oft angenommen wird, werden andere Aspekte vernachlässigt. Ende April 2019 konnten die Administratoren des weltweit zweitgrössten Darknet-Markts – dank der Auswertung der in der Blockchain verankerten Daten – festgenommen werden. Auch der Administrator des grössten deutschen Darknet-Forums «Deutschland im Deep Web» wurde enttarnt, weil die Ermittler den Weg der Gelder mittels Blockchain nachvollziehen konnten.[34] Indem die Blockchain-Technologie die in ihrem Netzwerk lückenlos registrierten Informationen und Transaktionen jederzeit belegen kann, verhält sie sich wie ein Dritter, der Zeuge für die Integrität der im Netzwerk gespeicherten Dateien und Informationen ist. Dank ihrer Eigenschaften kann die Blockchain-Technologie in kriminalistischer Hinsicht interessant werden und polizeiliche Ermittlungen wesentlich erleichtern. Dies setzt voraus, dass die Ermittler entsprechend geschult werden und mit Techniken und Methoden der Ermittlung relevanter Tatsachen, die etwa auf den Einsatz von Kryptowährungen hinweisen, vertraut sind. Die neuen Ermittlungsmethoden der Strafverfolgungsbehörden zeigt Furneaux (2018) am Beispiel der Kryptowährungen auf.[35] Die Blockchain-Technologie bringt somit in kriminalistischer Hinsicht nicht nur neue Risiken, sondern auch neue Chancen mit sich.

Zusammenfassend ist festzustellen, dass in der Schweiz zurzeit die rechtlichen Rahmenbedingungen für den Umgang mit der Blockchain-Technologie ausreichend sind. Jedoch gilt es, die rasanten Entwicklungen in diesem Bereich im Auge zu behalten, um allenfalls zeitnahe darauf reagieren zu können.

32 Siehe Janze, Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets, Twenty-third Americas Conference on Information Systems, Boston 2017.

33 Offenbar lässt sich der Umgang mit Kryptowährungen nicht ohne Weiteres anhand des Modells des «homo oeconomicus» erklären.

34 Siehe Dölle, Spurensicherung: Wie die Blockchain Kriminelle überführt, Beitrag vom 24.05.2019, abrufbar unter https://www.heise.de/ct/artikel/Spurensicherung-Wie-die-Blockchain-Kriminelle-ueberfuehrt-4427702.html, [01.10.2019]).

35 Furneaux, Investigating Cryptocurrencies, Understanding, Extracting, and Analyzing Blockchain Evidence, Indianapolis 2018, 117 ff.