www.jusletter.ch

Jana Essebier / Dominic A. Wyss

Von der Blockchain zu Smart Contracts

Der Begriff der Blockchain ist in aller Munde. Die Rede ist davon, dass er nicht nur die Finanzwelt, sondern auch das Recht ändern wird. Begriffe wie Smart Contracts und Coding Lawyers prägen die Diskussion. Der Beitrag gibt zunächst einen Überblick darüber, was es mit Blockchain und Smart Contracts auf sich hat. Anschliessend widmen sich die Autoren der Frage, ob tatsächlich eine Revolution des Rechts bevorsteht.

Beitragsarten: Beiträge
Rechtsgebiete: Immaterialgüterrecht; Medien- und Telekommunikationsrecht; Informatik und Recht; Kapitalmarktrecht; Aufsichtsrecht; Datenschutz; E-Commerce

Zitiervorschlag: Jana Essebier / Dominic A. Wyss, Von der Blockchain zu Smart Contracts, in: Jusletter 24. April 2017

Inhaltsübersicht

I. Was ist die Blockchain?

[Rz 1] Die Blockchain ist eine jedermann zugängliche (open source), softwarebasierte Technologie. Als Erfinder der Blockchain-Technologie gilt der nur unter dem Pseudonym Satoshi Nakamoto bekannte Erfinder von Bitcoin, einer virtuellen Währung.[1]

[Rz 2] Die Blockchain funktioniert wie eine dezentrale Datenbank. Diese Datenbank dokumentiert digital ausgeführte Transaktionen. Wie ein Logbuch oder ein Register erfasst die Datenbank chronologisch alle Transaktionen.[2] Der Begriff «Blockchain» steht dafür, dass die Daten in Form von sogenannten «blocks» aneinandergehängt, also gekettet («chain») werden.[3]

[Rz 3] Die Datenbank ist grundsätzlich öffentlich, d.h. jeder hat die Möglichkeit, sie einzusehen und Nutzer der Blockchain zu werden.[4] Die Blockchain funktioniert ohne eine zentrale Aufsicht oder einen Vermittler. Die Korrektheit der Datenbank wird daher nicht durch eine zentrale Stelle, sondern durch die Funktionsweise der Blockchain selbst sichergestellt.

---

1 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (abrufbar unter https://bitcoin.org/de/); Bitcoin wurde kurz nach dem Zusammenbruch von Lehman Brothers Ende 2008 eingeführt.

2 Government Office for Science, Distributed Ledger Technology, beyond block chain, 2016, S. 22 (abrufbar unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf; alle Websites zuletzt besucht am 3. April 2017).

3 Rolf H. Weber/Simone Baumann, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien, in: Jusletter 21. September 2015, S. 9 f.; Konrad Hummler, Blockchain – der nächste Wohlstandsschock, NZZ vom 3. Mai 2016, S. 27; siehe auch die kurze Darstellung in EFD, Änderung des Bankengesetzes und der Bankenverordnung (FinTech), Erläuternder Bericht zur Vernehmlassungsvorlage, 1. Februar 2017, S. 9 ff.

4 In der Praxis werden abweichend von diesem Grundmodell geschlossene Blockchain-Modelle entwickelt, bei denen nur bestimmte Nutzer Zugang erhalten, z.B. nur Banken. Z.T. wird hierfür in der Praxis auch der Begriff Distributed Ledger verwendet. Vgl. hierzu auch Javier Sebastian Cermeno, Blockchain in financial services: Regulatory landscape and future challenges for its commercial application, Working Paper December 2016, S. 3 (abrufbar unter https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf).

[Rz 4] Was einmal in der Blockchain dokumentiert ist, kann nicht nachträglich geändert werden. Dies lässt sich an folgendem Beispiel verdeutlichen:

[Rz 5] A möchte an B 10 Bitcoins übertragen. Er vertippt sich und tippt daher 100 Bitcoins ein. Auf der Blockchain ist daher eine Transaktion von 100 Bitcoins dokumentiert. Dies kann auch mit Zustimmung von B nicht nachträglich geändert werden. A und B müssen daher eine neue Transaktion abschliessen, um das Ergebnis zu korrigieren. B muss eine Übertragung von 90 Bitcoins an A vornehmen.

II. Wie funktioniert die Blockchain?

[Rz 6] Wie wird nun sichergestellt, dass die in der Blockchain gespeicherten Daten korrekt sind und korrekt bleiben? Woher weiss man, dass etwas tatsächlich der Person «gehört», die es behauptet? Vereinfacht dargestellt sind die folgenden Elemente der Blockchain-Technologie zentral:[5]

1. Verschlüsselung

[Rz 7] Um Daten in der Blockchain dokumentieren zu können, wird ein Konto eröffnet. Jeder Nutzer kann beliebig viele Konten errichten. Jeder Nutzer, dessen Daten in der Blockchain dokumentiert sind, verfügt über eine digitale Signatur, d.h. es gibt einen Private Key und einen Public Key. Mit Hilfe des Private Keys signiert der Nutzer die Nachricht und damit die Transaktion.[6] Diese digitale Signatur dient dazu, die Echtheit der Transaktion sicherzustellen. Nur korrekt signierte Transaktionen werden in die Blockchain aufgenommen.[7]

[Rz 8] Die Daten auf der Blockchain werden mittels einer sogenannten kryptographischen Hashfunktion verschlüsselt.[8] Die Hashfunktion erzeugt für jeden beliebigen Datensatz eine individuelle Zeichenfolge mit vorgegebener Länge.[9] Hashfunktionen sind nicht umkehrbare Verschlüsslungsfunktionen. Sie funktionieren wie Einbahnstrassen. Für jeden Datensatz kann mit einem gewissen Mass an Aufwand ein Prüfwert erstellt werden. Die Entschlüsselung ist hingegen gegenwärtig (nahezu) unmöglich.[10] Bildlich kann man sich dies wie ein Ei vorstellen. Aus einem Hühnerei lässt sich mit etwas Arbeit ein Rührei herstellen. Es ist hingegen nicht möglich, aus einem Rührei wieder ein Ei herzustellen.

[Rz 9] Hashfunktionen sollen sicherstellen, dass es für jeden Datensatz nur einen Prüfwert gibt. So wird sichergestellt, dass der Datensatz anhand des Prüfwerts eindeutig identifiziert werden kann, also sozusagen einen Fingerabdruck erhält.[11] Der Blockchain wird nur dann ein neuer Da-

---

5 Die Darstellung orientiert sich an Bitcoin.

6 Michael Crosby et al., BlockChain Technology, Beyond Bitcoin, Sutardja Center for Entrepreneurship and Technology Technical Report, Berkeley 16. Oktober 2015, S. 6 (abrufbar unter http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf); EFD FinTech (Fn. 3), S. 9 f.

7 Vgl. EFD FinTech (Fn. 3), S. 9 f.; Luisa Geiling, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, BaFin Journal Februar 2016, S. 28 f.

8 Zur Funktionsweise anhand von Beispielen vgl. z.B. http://hashgenerator.de.

9 Vgl. Crosby (Fn. 6), S. 6.

10 Vgl. Walter Blocher, The next big thing: Blockchain – Bitcoin –Smart Contracts, AnwBl 2016, S. 615; es bleibt abzuwarten, ob die weitere Entwicklung der Quantencomputer etwas an dieser Einschätzung ändert.

11 Vgl. EFD FinTech (Fn. 3), S. 9 f.; Weber/Baumann (Fn. 3), S. 9 f.; Hummler (Fn. 3), S. 27.

tenblock hinzugefügt, wenn der Datenblock verifiziert und verschlüsselt ist. Jeder Datenblock verfügt über einen Zeitstempel.

2. Dezentrale Datenbank

[Rz 10] Die Daten einer Transaktion werden in chronologischer Reihenfolge in Blöcken gespeichert, die durch die Hashwerte verbunden werden. Jeder Block enthält eine Kopie des vorhergehenden Datenblocks.[12] Wenn man somit einen Block nachträglich korrigieren möchte, dann müsste man somit alle vorhergehenden Blöcke bis hin zu jenem, den man tatsächlich korrigieren will, ändern. Dies erhöht den Aufwand für eine nachträgliche Manipulation substantiell. Die Transaktionen sind somit grundsätzlich unveränderlich in der Blockchain registriert und können nicht rückabgewickelt werden.[13]

[Rz 11] Schliesslich werden Kopien dieser Datenkette auf viele Rechner des Netzwerks verteilt und laufend aktualisiert. Die Rede ist von einem Distributed Ledger, einer dezentralen Datenbank.[14] Die längste Blockchain gilt jeweils als richtig. Wer die Blockchain verändern möchte, müsste auch die Kopien der Datenkette auf anderen Rechnern verändern. Selbst wenn ein Rechner aus dem System ausscheidet, funktioniert die Datenbank weiter. Dies gewährleistet die Sicherheit des Systems.[15] Die Technologie ist damit von einer zentralen, vertrauenswürdigen Instanz unabhängig.[16]

[Rz 12] In der Praxis sehen die Blockchain-Technologien nicht vor, dass die Datenkette auf allen Rechnern identisch ist, sondern es gilt das Mehrheitsprinzip. Angaben, die sich nicht in einer Mehrheit der geteilten bzw. dezentralisierten Register widerspiegeln, werden eliminiert. Aufgrund dieser kollektiven Verifizierung der Daten und ihrer Verschlüsselung gilt das Blockchain-System als unveränderbar und kaum fälschbar.[17]

3. Ist die Blockchain kostenlos?

[Rz 13] Eine Transaktion wird nicht für sich genommen der Blockchain beigefügt, sondern sie wird zusammen mit anderen Transaktionen zu einem Block zusammengefügt. Die Blockchain-Technologie enthält ein Protokoll, welches festlegt, welcher Block und in welcher Reihenfolge neue Blocks der Blockchain hinzugefügt werden. Dies wird auch als Consensus Protocol (Abstimmungsverfahren) bezeichnet.

---

12 Crosby (Fn. 6), S. 7 ff.

13 Vgl. EFD FinTech (Fn. 3), S. 9 f.; Blocher (Fn. 10), S. 615 f.; Weber/Baumann (Fn. 3), S. 9 f., 12; Luzius Meisser, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, S. 83, 86; Micha Roon, Schlichtung und Blockchain, Anwaltsrevue 2016, S. 359 ff.; Government Office for Science (Fn. 2), S. 33 ff.; Hummler (Fn. 3), S. 27.

14 Crosby (Fn. 6), S. 7 ff.; Blocher (Fn. 10), S. 615; Weber/Baumann (Fn. 3), S. 10.

15 Weber/Baumann (Fn. 3), S. 12; Geiling (Fn. 7), S. 31.

16 Vgl. Blocher (Fn. 10), S. 616; Government Office for Science (Fn. 2), S. 33 f.

17 Vgl. Meisser (Fn. 13), S. 82 ff.; Crosby (Fn. 6), S.11.

[Rz 14] Bitcoin basiert auf dem sogenannten Proof of Work-Protokoll.[18] Der Block wird dann der Blockchain hinzugefügt, sobald die Hashfunktion gelöst und der Block somit mit dem nötigen Prüfwert versehen wurde. Das Lösen der Hashfunktion wird durch sogenannte Miner übernommen. Sie verfügen über die nötige Computerleistung und erhalten als Entschädigung eine Gebühr in Bitcoin.[19] Zwar ist nicht ausgeschlossen, dass sie diese Tätigkeit auch ohne Gegenleistung ausüben. Dann kann es jedoch längere Zeit in Anspruch nehmen, bis die Transaktion in einen Block aufgenommen wird.

[Rz 15] Denkbar sind auch Methoden, welche ohne Entschädigungen funktionieren. Es stellt sich dann jedoch die Frage, welche Anreize für die Nutzer gesetzt werden, an den «Abstimmungsverfahren» teilzunehmen.

III. Welchen Zweck erfüllt die Blockchain?

1. Die Blockchain schafft Vertrauen

[Rz 16] Die Blockchain erlaubt es, Daten unveränderbar und in einer chronologischen Reihenfolge zu speichern. Die Funktionsweise der Blockchain stellt grundsätzlich sicher, dass über einen Vermögenswert nicht zweimal verfügt werden kann (sogenanntes Double Spending). Dies jedenfalls dann, wenn der Vermögenswert nur durch eine Transaktion über die Blockchain übertragen werden kann, sei es, weil er nur auf der Blockchain existiert (wie Kryptowährungen), sei es, dass ein Dritter sicherstellt, dass über den physischen Vermögenswert nicht ohne entsprechende Blockchaintransaktion verfügt werden kann.

[Rz 17] Die Blockchain kann daher zu Beweiszwecken dienen. Sie erlaubt es Personen, allein im Vertrauen auf die Technologie miteinander Transaktionen einzugehen. Denn diese Personen sollen darauf vertrauen können, dass die Blockchain wie ein Prüfprotokoll funktioniert und somit korrekt dokumentiert, wem ein Vermögenswert «gehört». Man spricht von einer Automatisierung des Vertrauens.[20] Verbunden damit ist der mögliche Verzicht auf Intermediäre. Das Vertrauen in den Intermediär soll durch das Vertrauen darin, dass die Blockchain verlässlich funktioniert und korrekt ist, ersetzt werden. Vertrauen verliert mit der Blockchain nicht seine Bedeutung, sondern verlagert sich. Es bezieht sich neu auf die Verlässlichkeit einer Technologie und nicht einer Person oder Institution.

[Rz 18] Die Blockchain kann daher dazu dienen, digital Vermögenswerte und Rechte, welche dann zwischen Parteien auf der Blockchain ausgetauscht werden können, zu repräsentieren. Möglich ist es auch, die Information auf der Blockchain mit einem verbindlichen Versprechen eines Dritten zu verbinden, welcher zusagt, gegen Übertragung sogenannter digitaler Tokens die tatsächlichen physischen Vermögenswerte auf die berechtigte Person zu übertragen (auch als Colored Coin bezeichnet). Der digitale Token ist somit mit einem Wertpapier vergleichbar.[21] Diese

---

18 Andere Methoden sind z.B. Ripple Protokoll, Proof of Stake und Proof of Elapsed Time; vgl. dazu ENISA, Distributed Ledger Technology & Cybersecurity, December 2016 (abrufbar unter https://ec.europa.eu/futurium/en/system/files/ged/wp2016_3-1_4_blockchain_security.pdf).

19 Miner kann grundsätzlich jeder sein, der über die nötige Computerleistung verfügt. Durch eine genügend hohe Entschädigung wird dafür gesorgt, dass es genügend Personen gibt, welche als Miner tätig sein wollen.

20 Roon (Fn. 13), S. 362; Blocher, (Fn. 10), S. 615 («Ersatz von sozialem Vertrauen oder Systemvertrauen durch ein Protokoll»); zur Beweisfunktion Mirjam Eggen, Chain of Contracts, AJP 2017, S. 12 ff.

21 Vgl. Weber/Baumann (Fn. 3), S. 11; Meisser (Fn. 13), S. 90 f.; Eggen (Fn. 20), S. 6.

Funktion ermöglicht es, die Blockchain-Technologie für Transaktionen mit physischen Vermögensgegenständen zu verwenden.[22]

2. Effizienz

[Rz 19] Die Blockchain-Technologie soll es ermöglichen, Transaktionen günstiger, sicherer und rascher abzuwickeln. Kosten sollen unter anderem durch den Verzicht auf Intermediäre gespart werden.[23] Zwar ist auch der Einsatz der Blockchain-Technologie, wie dargestellt, nicht kostenlos, dennoch sind erhebliche Kostenreduktionen denkbar. Dadurch, dass die Blockchain dokumentiert, wem etwas «gehört», könnte zudem auf aufwändige Prüfungen verzichtet werden. Ob die Transaktionen tatsächlich rascher als bisher abgewickelt werden können, hängt vom Einzelfall ab. Häufig dürfte dies der Fall sein. Der Schnelligkeit sind jedoch durch die Technologie selbst Grenzen gesetzt. Abzuwarten bleibt zudem, inwiefern traditionelle Methoden, wie z.B. die bisherigen Zahlungs- und Wertpapierabwicklungssysteme, durch den Wettbewerbsdruck effizienter werden.

[Rz 20] Zu erwähnen ist hier ein weiteres Problem der Blockchain. Die Blockchain verbraucht insgesamt substantiell Energie, da Daten auf einer Vielzahl von Rechnern kopiert und abgespeichert werden. In der Praxis wird jedoch davon ausgegangen, dass sich dieses Problem durch die zukünftige Weiterentwicklung der Technologie lösen lässt.

IV. Ausgewählte Risiken der Blockchain

[Rz 21] Die Blockchain-Technologie ist neu und die Umsetzung noch in den Anfängen begriffen. Chancen und Risiken lassen sich daher erst in Grundzügen erfassen. Die Europäische Agentur für Netz-und Informationssicherheit hat im Dezember 2016 einen Bericht publiziert, der sich mit den Herausforderungen auseinandersetzt und erste Möglichkeiten zum Umgang mit diesen Risiken aufzeigt.[24]

[Rz 22] Zu diesen Risiken gehören insbesondere Folgende:

1. Verlust des Private Key

[Rz 23] Sollten unberechtigte Dritte Zugang zum Private Key erhalten, können sie grundsätzlich über die Vermögenswerte verfügen, welche in der Blockchain dokumentiert sind. Sollte der Nutzer den Private Key verlieren, verliert er seinen Zugang zur Blockchain und damit faktisch für immer die Verfügungsmöglichkeiten über die in der Blockchain dokumentierten Vermögenswerte. Denn bei der Blockchain gibt es keine zentrale Ansprechperson, welche die Einstellungen wieder zurücksetzen und einen neuen Private Key ausgeben könnte. Aufgrund der unumkehrba-

22 Geiling (Fn. 7), S. 31; siehe zum Ganzen Rosenfeld, Overview of Colored Coins, 4. Dezember 2012; zum Übertragungssystem aus zivilrechtlicher Sicht Eggen (Fn. 20), S. 12 ff.

23 Weber/Baumann (Fn. 3), S. 10.

24 ENISA, Distributed Ledger Technology & Cybersecurity, December 2016 (abrufbar unter https://www.enisa.europa.eu/https://www.enisa.europa.eu/).

ren Folgen eines Verlusts des Private Keys ist es denkbar, dass die Verwahrung und Verwaltung von Private Keys ein neues Geschäftsfeld für Intermediäre darstellen kann.

2. Vertrauensverlust

[Rz 24] Vertrauen ist zentral für die Zweckerfüllung der Blockchain. Medienmitteilungen oder Gerüchte darüber, dass Blockchains gehackt wurden oder Fehler aufweisen, stellen immer auch die Existenzberechtigung der Blockchain in Frage. Wenn Nutzer kein Vertrauen mehr in die Blockchain haben, dann verlieren auch auf der Blockchain repräsentierte digitale Vermögenswerte und Rechte an Wert, sofern es dem Nutzer nicht gelingt, die Rechtszuständigkeit auch ausserhalb und ohne Blockchain nachzuweisen.

V. Anwendungsbereiche der Blockchain

[Rz 25] Die Blockchain-Technologie kann für eine Vielzahl von Anwendungen eingesetzt werden. Sie ist mithin eine Infrastruktur, auf der die jeweilige Anwendung basiert bzw. abgewickelt wird. In der Praxis wird die Blockchain nie als Selbstzweck bestehen, sondern immer mit einer konkreten Anwendung verknüpft sein.

[Rz 26] Der bekannteste Anwendungsbereich der Blockchain ist weiterhin Bitcoin. Obwohl mittlerweile mehr als 600 weiterer solcher Systeme bestehen, ist Bitcoin nach wie vor am populärsten.[25] Virtuelle Währungen digitalisieren den physischen Barzahlungsvorgang und ermöglichen diesen auf Distanz, ohne dass Intermediäre erforderlich sind.[26] Damit sind Zahlungen direkt zwischen zwei Privatpersonen möglich. Den virtuellen Währungen ist eigen, dass sie nicht von einer Zentralbank oder öffentlichen Stelle emittiert werden. Es sind digitale Daten, die einen Wert darstellen, jedoch kein offizielles Zahlungsmittel sind und auch nicht auf dem gesetzlichen Zahlungsmittel basieren.[27]

[Rz 27] Das Hauptanwendungsgebiet der Blockchain-Technologie ausserhalb der virtuellen Währungen wird vielfach im Bereich der Finanzdienstleistungen (FinTech) gesehen. Genannt werden insbesondere Anwendungen wie (internationale) Zahlungs- und Finanztransaktionen, Wertpa-

---

25 Europäisches Parlament, Bericht über virtuelle Währungen, S. 5; vgl. Seraina Grünewald, Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, S. 94; Meisser (Fn. 13), S. 89; von den dezentral organisierten Systemen unterscheiden sich zentral verwaltete virtuelle Währungen, bei welchen eine zentrale Instanz aus Währungsausgeber und Systembetreiber auftritt. Solche zentrale Systeme sind nicht Gegenstand des vorliegenden Artikels.

26 Vgl. Government Office for Science (Fn. 2), S. 33.

27 Siehe auch Definition im Bericht des Bundesrats zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, S. 7 ff.; Europäisches Parlament, Bericht über virtuelle Währungen vom 3. Mai 2016, S. 5; European Parliamentary Research Service (EPRS), Briefing March 2016, Virtual currencies, S. 4; European Central Bank, Virtual currency schemes – a further analysis, Februar 2015, S. 4; für weitere Definitionen Harald Bärtschi/Christina Meisser, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, S. 115; Grünewald (Fn. 25), S. 93; Weber/Baumann (Fn. 3), S. 8 f.; zur Geldfunktion Bärtschi/Meisser (Fn. 27), S. 142 f.

pierclearing und -abrechnung.[28] Ein weiteres Beispiel ist der Bereich von Private Equity-Investitionen. Hier könnte die Blockchain den Sekundärhandel erleichtern.

[Rz 28] Zahlreiche Anwendungen sind auch ausserhalb des Finanzdienstleistungssektors denkbar. Die Blockchain kann das Eigentum an Vermögenswerten dokumentieren und könnte zur Eigentumsübertragung von beliebigen Vermögenswerten verwendet werden. Wer Vertrauen in die Blockchain hat, vertraut darin, dass die Blockchain korrekt dokumentiert, wer Eigentümer ist.[29] Denkbar ist somit, dass die Blockchain für die Dokumentation, wer Eigentümer eines Kunstwerks ist, verwendet wird. Ein anderes Beispiel ist der Gebrauchtwarenhandel. So liesse sich der Erwerb von gestohlener Ware vermeiden. Gegen Fälschungen liesse sich dadurch vorgehen, dass z.B. eine Originaluhr über einen Chip auf einer Blockchain registriert wird. Denkbar ist, dass die Blockchain zum Ersatz für zentrale Register, wie für Immaterialgüterrechte und das Grundbuch, werden könnte.

VI. Smart Contracts

[Rz 29] Die Blockchain kann grundsätzlich bei Verträgen verwendet werden, deren Abschluss und Abwicklung heute weitgehend auf Vertrauen basiert. Hierbei können sogenannte Smart Contracts eingesetzt werden.

1. Was sind Smart Contracts?

[Rz 30] Der Begriff der Smart Contracts wurde soweit ersichtlich erstmals 1997 von Nick Szabo einem Informatiker und Juristen verwendet.[30]

[Rz 31] Smart Contracts sind sich selbst ausführende oder selbst vollziehende Verträge, die in einer Blockchain gespeichert und repliziert werden können. Die Vertragsbestimmungen werden direkt in einem Code, also einem Computerprogramm, abgebildet. Die vordefinierten Vertragsregeln werden dann von einem Computer automatisch ausgeführt. Je nach Programmierung können damit Vertragsteile oder der gesamte Vertrag automatisiert werden.[31] Voraussetzung ist, dass das Computerprogramm automatisch prüfen kann, ob die Parteien ihre Verpflichtungen erfüllen.

[Rz 32] Grundsätzlich kann eine Blockchain nur auf die Daten zugreifen, welche innerhalb der Blockchain vorliegen. Bei Smart Contracts ist es häufig nötig, externe Ereignisse zu berücksichtigen. Dies geschieht durch sogenannte Orakel. Orakel können sowohl automatisierte Dateneingaben als auch vertrauenswürdige, unabhängige Dritte sein, welche bestimmte Entscheidungen treffen können oder müssen. Damit lassen sich mit der Blockchain-Technologie zukünftige Ereignisse abbilden.[32]

---

28 Luca Bianchi/Edi Bolliger, A (Legal) Perspective on Blockchain, CapLaw 2016; Allens/Linklaters, Blockchain Reaction, S. 8.

29 Crosby (Fn. 6), S. 14.

30 http://firstmonday.org/ojs/index.php/fm/article/view/548; Crosby (Fn. 6), S. 11.

31 Siehe zum Ganzen Government Office for Science (Fn. 2), S. 22 ff.; Eggen (Fn. 20), S. 6.

32 Orakel erhöhen jedoch damit auch das Manipulationsrisiko; zu Orakel vgl. Allen/Linklaters (Fn. 28), S. 14.

[Rz 33] Die Funktionsweise von Smart Contracts ist nicht neu und besteht beispielsweise bei Warenautomaten bereits seit vielen Jahren. Mit den neuen technologischen Möglichkeiten sind nun aber weitaus komplexere Anwendungsmöglichkeiten denkbar. Beispiele sind:

- Ein Musikverleiher kann die Rechte an bestimmten Musikstücken in einer Blockchain dokumentieren. Die Software könnte vorsehen, dass derjenige die Musik runterladen darf, der im Gegenzug mittels der Blockchain eine Zahlung an den Musikverleiher leistet. Zudem könnte der Code vorsehen, dass nur eine Teilzahlung vorzunehmen ist, wenn der Nutzer nach der Hälfte des Musikstücks entscheidet, es nicht weiterzuhören. Die Abwicklung würde jeweils automatisch geschehen.
- In Brooklyn wird der Einsatz der Blockchain bei lokalen Mikrostromnetzen getestet. Mit Hilfe der Blockchain kann hier automatisch dokumentiert werden, wer wann wieviel Strom produziert und verbraucht, ohne dass es hierfür eine zentrale Überwachungsstelle benötigen würde.[33]
- Die Berechtigung an einer Versicherungspolice könnte in der Blockchain dokumentiert werden. Zugleich könnte ein Code vorsehen, wann Auszahlungen zu erfolgen haben. Denkbar wäre, dass ein neutraler Dritter jeweils feststellt, ob ein bestimmtes Ereignis vorliegt, so dass der Code zur Auszahlung führt.
- Ein anderes Beispiel ist die Verwendung der Blockchain für die Abwicklung von Zahlungen auf Wertschriften. So könnte die Blockchain dokumentieren, wer Aktien oder Anleihen hält. Der Code könnte vorsehen, dass automatisch Zinsen oder Dividenden an diese Nutzer gezahlt werden. Die Zinsen liessen sich auf diese Weise stunden- oder sogar sekundengenau abrechnen.

[Rz 34] Da die Vertragsregeln in einem Code niedergelegt sind, ist auch die Rede von «Coding Lawyers», sobald Anwälte diese Computerprogramme gemeinsam mit Programmierern schreiben.

2. Was sind die Vorteile bei Smart Contracts?

[Rz 35] Sämtliche Nutzer eines Blockchain-Netzwerkes verfügen über eine Kopie des Vertragscodes und sorgen dafür, dass der Vertrag nicht einseitig abgeändert werden kann. Ausserdem vollziehen sich – im Idealfall – die vereinbarten Leistungen beim Vorliegen der vordefinierten und vereinbarten Voraussetzungen automatisch. Dies erhöht die Geschwindigkeit sowie die Sicherheit und reduziert gleichzeitig die Kosten und die operationellen Risiken.

[Rz 36] Die Leistungen können, wenn die vordefinierten Voraussetzungen erfüllt sind, nicht mehr grundlos oder böswillig verweigert werden. Dadurch ermöglichen Smart Contracts auch Geschäfte zwischen Parteien, die sich nicht vertrauen. Die Anzahl potenzieller Geschäftskunden würde sich für ein Unternehmen damit schlagartig vervielfachen.

[Rz 37] Darüber hinaus bestehen grundsätzlich keine Schwierigkeiten bei der Auslegung einer Vertragsklausel. Der Code vollzieht diese automatisch und strikt nach den vorgegebenen Regeln, ohne Interpretationsspielraum. Die Rechtsunsicherheit, die dem Abschluss von Verträgen entgegensteht, wäre somit eliminiert. Dies zumindest in der Theorie.

33 http://brooklynmicrogrid.com/.

[Rz 38] Die Blockchain protokolliert die mit dem Smart Contract verbundenen Transaktionen, z.B. bereits erfolgte Zinszahlungen. Die Vertragserfüllung kann damit stets nachvollzogen werden.

3. Welche rechtlichen Fragen stellen sich bei Smart Contracts?

[Rz 39] Ein Smart Contract ist gerade nicht «smart», sondern folgt seiner Programmierung. Der Code kann und darf nachträglich nicht mehr angepasst werden. Gerade der strikte Vollzug bzw. die strikte Ausführung von Smart Contracts ist rechtlich nicht unproblematisch. Die Unabänderbarkeit des definierten Codes sowie dessen starrer Vollzug können zu Ergebnissen führen, die keine der Parteien so gewollt hat bzw. die im Einzelfall nicht angemessen sind. Ermessen – ein wichtiger Bestandteil vieler Vertragsklauseln und ein Instrument, um dem Einzelfall gerecht zu werden – ist im Grundsatz in einem Smart Contract nicht vorgesehen. Dies führt zu unzähligen Fragen an der Schnittstelle zwischen Recht und Technik, welche im Code adressiert und gelöst werden müssen.

[Rz 40] Auf Smart Contracts findet das geltende Zivilrecht Anwendung. Ob ein Vertrag schriftlich, mündlich oder auf einer Blockchain abgeschlossen wurde, ist hierfür irrelevant. Die Frage, welches Recht auf einen Vertrag anwendbar sein soll, der dezentral und mit grosser Wahrscheinlichkeit auf Servern in einer Vielzahl von Rechtsordnungen abgespeichert ist, sowie die Frage des Gerichtstandes sind offen. Als Leitlinien können folgende gelten:

- Viele Rechtsordnungen sehen vor, dass auf einen Vertrag, mangels Rechtswahl, das Recht desjenigen anzuwenden ist, der die charakteristische Leistung erbringt. Dies dürfte in der Regel der Verwender sein.
- Setzt die Teilnahme an der konkreten Blockchain voraus, dass einer Rechtswahl zugestimmt wird, dann könnte vertreten werden, dass diese Rechtswahl auch für den einzelnen Smart Contract gilt.
- Werden Smart Contracts mit Konsumenten abgeschlossen, dürften die Gerichte das jeweilige zwingende Recht am Wohnsitz des Konsumenten durchsetzen.
- Führt der Smart Contract für den Konsumenten zu überraschenden Ergebnissen, z.B. weil er mit unvorhergesehenen Ereignissen nicht umgehen kann, könnten die Gerichte in den Smart Contracts verankerte Bedingungen als überraschende und damit unwirksame Allgemeine Geschäftsbedingungen ansehen.

[Rz 41] Weiter stellen sich neue haftungsrechtliche Fragen. Wer ist beispielsweise haftbar für einen fehlerhaften Code? Dabei kann bereits zweifelhaft sein, wann ein Code überhaupt fehlerhaft ist. So könnten die Anwender geltend machen, dass sie den Code entsprechend seiner Funktion korrekt angewendet hätten.[34] Haftet der Programmierer, der Verwender oder haften beide? Welche Rechtsfolgen haben Störungen bei Leistungen, die basierend auf der Blockchain-Technologie automatisch hätten erbracht werden sollen? Was passiert, wenn der Code zwingendes Recht nicht einhält und wer trägt dafür die Verantwortung?

34 Vgl. Allen/Linklaters (Fn. 28), S. 14; mit Etherum hat dieses Beispiel bereits einen Präzedenzfall: «Der unbekannte Hacker fand das unfair: In einem offenen Brief schrieb offenbar er persönlich, er habe nur ein explizit programmiertes Feature genutzt. Seine Anwaltskanzlei habe ihm beschieden, dass sein Tun mit amerikanischem Recht voll vereinbar sei.» (https://www.nzz.ch/wirtschaft/blockchain-der-schweizer-ethereum-stiftung-ein-suendenfall-als-antwort-auf-einen-hacker-ld.110502).

4. Revolution des Rechts?

[Rz 42] Aufgrund ihrer Funktionsweise bedeuten Smart Contracts eine Abkehr von der bisherigen Rechtspraxis:

- 99% aller Verträge werden in der Praxis mangels Streitfall nie relevant. Selbst wenn die Verhaltensweise nicht im Einklang mit dem Vertrag steht, ist dies unproblematisch, solange die Parteien sich einig sind. In vielen Fällen werden die Parteien daher nie erfahren, ob der Vertrag tatsächlich ihre Einigung korrekt wiedergab, ob es überhaupt bei Vertragsschluss eine solche Einigung gab, ob der Vertrag alle nötigen Punkte geregelt hat etc. Es ist zum Teil gerade diese Flexibilität der Parteien, die eine jahrelange, gut funktionierende Vertragsbeziehung ermöglicht.[35]
- Das geltende Privatrecht geht grundsätzlich davon aus, dass sich Parteien vertragsgemäss verhalten. Gerichte oder Schlichtungen werden erst dann angerufen, wenn sich eine Partei nicht vertragsgemäss verhält. Da dies nur selten der Fall ist oder das abweichende Verhalten von der anderen Vertragspartei toleriert wird, ist die Anrufung der Gerichte in einer Vertragsbeziehung die Ausnahme.

[Rz 43] Mit der Einführung von Smart Contracts ändert sich dies.

[Rz 44] Nun gilt, dass, wenn jemand von einem vertraglichen Recht Gebrauch machen möchte, das Computerprogramm jeweils prüft, ob er das auch darf. Das bedeutet zum einen, dass der Vertrag so exakt formuliert werden muss, dass dies möglich ist. Fehler bei der Vertragsgestaltung haben unmittelbare Konsequenzen. Zugleich steigt die Wahrscheinlichkeit, dass ein Gericht oder eine Schlichtung z.B. in Form eines Smart Oracles in Anspruch genommen werden muss.

[Rz 45] Die Konsequenzen lassen sich an einem einfachen Beispiel aufzeigen:

[Rz 46] A hat ein Auto von B geleast. Gemäss Vertrag muss er monatlich die Leasingrate überweisen. Haben A und B einen normalen Vertrag abgeschlossen und A überweist die Leasingrate nicht fristgemäss, kann A zunächst einmal das Auto weiter benutzen. Es obliegt B gegen A vorzugehen.

[Rz 47] Ein Smart Contract würde so ausgestaltet, dass der Autoschlüssel nur funktioniert, wenn die Blockchain jeweils die Information enthält, dass die Leasingrate überwiesen wurde. Zahlt A nicht fristgemäss, kann er das Auto nicht mehr benutzen. Das gleiche gilt, wenn A zwar fristgemäss gezahlt hat, aufgrund technischer Probleme die Zahlung jedoch nicht entsprechend verbucht wurde. Es obliegt in diesen Fällen A gegen B vorzugehen.

[Rz 48] Wenn A dem B mitgeteilt hätte, dass er zwei Wochen später zahlen wird, und B dagegen keine Einwände hätte, dann bestünde bei einer normalen Vertragsbeziehung kein Handlungsbedarf. Wenn die Parteien einen Smart Contract abgeschlossen hätten, würde das Auto jedoch auch dann nicht mehr funktionieren, wenn B keine Einwände hätte. A und B müssten daher grundsätzlich einen neuen Smart Contract abschliessen.

5. Keine vollständige Automatisierung von Vertragsbeziehungen

[Rz 49] Smart Contracts werden nie zu einer vollständigen Automatisierung führen, selbst wenn sämtliche Fehler bei der Vertragsgestaltung und Programmierung eliminiert werden könnten.

35 Vgl. Allen/Linklaters (Fn. 28), S. 14.

Dies ist insbesondere darauf zurückzuführen, dass es nie möglich sein wird, sämtliche zukünftigen Ereignisse zu antizipieren und im Code des Smart Contracts entsprechend zu hinterlegen. Selbst bei sehr einfachen Verhältnissen kann etwas Unvorhergesehenes passieren. Bei komplexen Verhältnissen steigt die Wahrscheinlichkeit. Für das Massengeschäft können Smart Contracts jedoch zu einer effizienten Lösung werden.

VII. Finanzmarktaufsichtsrecht

[Rz 50] Wie dargestellt, ist die Blockchain eine Technologie. Es ist somit nicht die Blockchain an sich, die zu einer Anwendung des Finanzmarktaufsichtsrechts führt, sondern die konkrete Einsatzmöglichkeit. Dies gilt vorrangig in Anwendungsbereichen mit Bezug zu Finanzdienstleistungen:[36]

- So könnte eine Blockchain die Basis für ein Zahlungssystem sein. Eine Bewilligungspflicht für Zahlungssysteme besteht nur ausnahmsweise.[37]
- Die Blockchain könnte die Grundlage für ein Effektenabwicklungssystem bilden, das bewilligungspflichtig ist.[38]
- Eine zentrale Verwahrungsstelle von Wertschriften und Wertrechten bedarf einer Bewilligung.[39] Fraglich ist, ob Wertschriften auf einer Blockchain tatsächlich «zentral verwahrt» würden. Dagegen spricht, dass es gerade nicht eine zentrale Stelle gibt, welche für die Verwahrung zuständig ist.
- Unter geltendem Recht sind virtuelle Währungen keine gesetzlichen Zahlungsmittel[40] und kein Buchgeld, das auf derselben Recheneinheit wie die gesetzlichen Zahlungsmittel basiert und durch die Mindestreservevorschriften reguliert ist.[41] Die Schaffung und Ausgabe von virtuellen Währungen ist nach Schweizer Recht bewilligungsfrei zulässig.[42] Gewisse Geschäftsmodelle erfordern beispielsweise eine Bankenbewilligung. Dies kann insbesondere dann der Fall sein, wenn beim Wechsel von virtuellen in offizielle Währungen und umgekehrt gewerbsmässig Geld oder Bitcoins von Kunden auf eigenen Konten entgegengenommen werden.[43] Denkbar ist dabei die Anwendbarkeit der Ausnahmebestimmung für Abwicklungskonten,[44] wobei die zulässige Haltedauer nach Vorschlag des Eidgenössischen Finanzdepartements (EFD) auf 60 Tage verlängert werden soll.[45]

---

36 Bei den Bewilligungspflichten nach Finanzmarktinfrastrukturgesetz (FinfraG) ist immer eine juristische Person nach Schweizer Recht erforderlich (Art. 8 FinfraG).

37 Art. 4 Abs. 2 FinfraG; Martin Liebi/Guenther Dobrauz, The current state of regulation of blockchain operations used in the financial industry in Switzerland, PWC (abrufbar unter http://news.pwc.ch/wp-content/uploads/2016/02/en_current-state-of-regulation_blockchain_financial-industry_switzerland.pdf), S. 3.

38 Art. 4 Abs. 1 i.V.m. Art. 2 lit. a FinfraG.

39 Art. 4 Abs. 1 i.V.m. Art. 2 lit. a FinfraG.

40 Siehe insbesondere Art. 2 Bundesgesetz über die Währung und die Zahlungsmittel (WZG); die Schaffung und Ausgabe von gesetzlichen Zahlungsmitteln steht allein dem Bund zu; siehe zum Ganzen Bärtschi/Meisser (Fn. 27), S. 117; Grünewald (Fn. 25), S. 97 ff.

41 Vgl. Bericht des Bundesrats (Fn. 27), S. 7.

42 Bärtschi/Meisser (Fn. 27), S. 123 ff.; Grünewald (Fn. 25), S. 99.

43 Bericht des Bundesrats (Fn. 27), S. 13; FINMA, Faktenblatt Bitcoins vom 25. Juni 2014.

44 Art. 5 Abs. 3 lit. c Bankenverordnung (BankV).

45 EFD FinTech (Fn. 3), S. 36.

- Auch wenn keine Bankenbewilligung erforderlich ist, können gewerbsmässige Tätigkeiten mit virtuellen Währungen dem Geldwäschereigesetz unterstehen, womit der Anschluss an eine Selbstregulierungsorganisation (SRO) bzw. die Direktunterstellung bei der FINMA erforderlich ist sowie die Sorgfaltspflichten gemäss GwG anwendbar werden.[46] Diesem Umstand trägt auch Art. 52 i.V.m. Art. 2 lit. c Geldwäschereiverordnung-FINMA (GwV-FINMA) Rechnung, indem Händler von virtuellen Währungen den Sorgfaltspflichten unterstellt sind.[47]

[Rz 51] Bewilligungspflichten können jedoch nicht nur bei Anwendungen mit Bezug zu Finanzdienstleistungen, sondern auch darüber hinaus entstehen. Im Mittelpunkt steht dabei die Frage, ob Colored Coins als Effekten oder Derivate qualifizieren, womit Tätigkeiten eine Bewilligung als Effektenhändler, Handelsplatz oder organisiertes Handelssystem erfordern könnten.

VIII. Ausblick

1. Ein neues weltweites Netzwerk?

[Rz 52] Die Blockchain-Technologie kann Nutzer weltweit miteinander verbinden. Gegenwärtig gibt es nicht nur eine einzige Blockchain, sondern viele verschiedene. Diese Blockchains weichen in den technischen Details voneinander ab, auch wenn viele auf dem Code basieren, welcher für Bitcoin verwendet wird. Noch sind Blockchains in der Entwicklungsphase. Erste Anwendungen in der Praxis führen zu neuen Erkenntnissen, welche wiederum zu Verbesserungen der Technologie führen.

[Rz 53] Eine Stärke der Blockchain-Technologie liegt in ihrer freien Zugänglichkeit, der dezentralen Natur und Unabhängigkeit. Diese Eigenschaften sind wichtige Anforderungen an Technologien, die als Plattform dienen.[48] Vielleicht wird sich aus den Blockchains daher ein weltweites Netzwerk entwickeln, welches die Nutzer, so wie heute das Internet, als Standard betrachten werden und welches die Art und Weise, wie wir Geschäfte miteinander tätigen, fundamental verändern wird. Die Rede ist gar von einem weltumspannenden «Internet of Value».[49]

2. Muss der Gesetzgeber handeln?

[Rz 54] Der Bundesrat hat das EFD beauftragt, einen Bericht unter anderem zum Handlungsbedarf im Bereich Blockchain auszuarbeiten. Ein entsprechender Bericht wird für Ende 2017 erwartet.

[Rz 55] Nach Auffassung der Autoren besteht kein Grund, die Blockchain als Technologie an sich zu regulieren. Grundsätzlich ist davon auszugehen, dass zivilrechtliche Fragen auf der Basis des geltenden Rechts beantwortet werden können. Die Praxisanwendungen befinden sich momentan

---

46 Bericht des Bundesrats (Fn. 27), S. 15; FINMA, Faktenblatt (Fn. 43); Grünewald (Fn. 25), S. 102 ff.

47 Weber/Baumann (Fn. 3), S. 9. Je nach Ausgestaltung der virtuellen Währung insbesondere in Bezug auf den Anonymitätsgrad der Nutzer bestehen hier Schwierigkeiten. Ein möglicher Regulierungsansatz würde wohl beim Wechsel von virtuellen in offizielle Währungen bestehen, vgl. European Parliamentary Research Service (Fn. 27), S. 6 ff.; Government Office for Science (Fn. 2), S. 34.

48 Vgl. Meisser (Fn. 13), S. 89 f.

49 The Economist, Blockchain – The next big thing, Or is it?, 9. Mai 2015 (abrufbar unter www.economist.com/node/21650295).

in der Experimentierphase, in welcher ein besseres Verständnis für die Technologie und deren Grenzen gewonnen werden soll.[50] Erst wenn sich in der Praxis zeigen sollte, dass sich bestimmte Fragen häufiger stellen und auf der Basis des geltenden Rechts nicht angemessen behandelt werden können, sollte der Gesetzgeber eine spezifische Regelung prüfen. Solche Fragen könnten sich insbesondere dann stellen, wenn die Blockchain zur Dokumentation des Eigentums an Wertschriften genutzt wird. Der Bundesrat hat bereits festgehalten, dass er die Entwicklungen im Bereich Blockchain in Zukunft eng mitverfolgen und bei Bedarf die notwendigen regulatorischen Anpassungen rasch vorschlagen wird.[51]

[Rz 56] Soweit regulierte Finanzmarktteilnehmer auf die Blockchain als Technologie zurückgreifen, bietet die Beaufsichtigung des Instituts eine Grundlage, um auch die Verwendung der Blockchain zu überprüfen.[52] Sollte die Blockchain-Technologie als Ersatz für das bisherige Zentralverwahrungssystem in Betracht gezogen werden, wäre eine Überprüfung der bestehenden Regulierung zu wünschen, um Systemrisiken auszuschliessen. Insbesondere wird dabei auch die Frage zu beantworten sein, wie der Gesetzgeber bzw. die Aufsichtsbehörden damit umgehen, dass es bei dezentralen Systemen keinen Ansprechpartner bzw. keinen Bewilligungsträger mehr geben könnte.[53]

[Rz 57] In der Schweiz bestehen nur punktuell spezifische Regelungen für virtuelle Währungen.[54] Es ist den Parteien im Rahmen der privatrechtlichen Freiheiten unbenommen, virtuelle Währungen als Zahlungsmittel zu vereinbaren.[55] Die Nutzung der virtuellen Währungen löst dabei weder bei der zahlenden noch bei der bezahlten Person Bewilligungspflichten aus.[56] Dies sollte nach Ansicht der Autoren auch nicht geändert werden. Der Fokus sollte stattdessen auf der Aufklärung der Marktteilnehmer über die Eigenschaften von Kryptowährungen liegen. Zum heutigen Zeitpunkt ist soweit ersichtlich auch keine spezifische Regulierung von virtuellen Währungen geplant.[57] Jedoch könnten Dienstleister im Bereich der virtuellen Währungen von den vom Bundesrat geplanten Erleichterungen für innovative Finanztechnologien (Fintech) profitieren.[58]

[Rz 58] Für Rechtsunsicherheit sorgt im Bereich der Kryptowährungen die Frage, ob an virtuellen Währungen ein Eigentumsrecht besteht oder ob es sich ausschliesslich um relative Rechte handelt. Die Diskussion, ob an Kryptowährungen und anderen digitalen Daten ein Eigentumsrecht bestehen kann, steht in der Schweiz noch ganz am Anfang.[59] Nach bisher wohl überwiegender

---

50 Allen/Linklaters (Fn. 28), S. 10; siehe auch Karsten Seibel, Blockchain ist die Revolution des Geldverkehrs, Welt vom 22. Oktober 2015 (abrufbar unter https://www.welt.de/wirtschaft/article147906848/Blockchain-ist-die-Revolution-des-Geldverkehrs.html).

51 Medienmitteilung des Bundesrats vom 2. Februar 2017 (abrufbar unter https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-65476.html).

52 Für die Revisionsstellen und Aufsichtsbehörden stellt sich hier jedoch ein technisches Problem – die Frage, wie Blockchains in der Praxis geprüft werden können.

53 Weber/Baumann (Fn. 3), S. 13.

54 Vgl. Weber/Baumann (Fn. 3), S. 8.

55 Bericht des Bundesrats (Fn. 27), S. 7, 10; zur Frage, ob die entsprechenden Schulden alternativ mit Schweizer Franken beglichen werden können Bärtschi/Meisser (Fn. 27), S. 146 f., 151.

56 Bericht des Bundesrats (Fn. 27), S. 13 ff.; FINMA Faktenblatt (Fn. 43).

57 Bericht des Bundesrats (Fn. 27), S. 13 ff.

58 Siehe nachstehend.

59 Florent Thouvenin, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, S. 22; Martin Eckert, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, S. 245 ff.; ablehnend Bärtschi/Meisser (Fn. 27), S. 141 f.; BJ, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über

Meinung bestehen an virtuellen Währungen nur relative Rechte. Ein Schutz der fraglichen Vermögenspositionen kann sich unter geltendem Recht allenfalls aus dem Recht der unerlaubten Handlung (Schadenersatz) oder aus dem Bereicherungsrecht ergeben.[60] Der Bundesrat hat nun angekündigt, sich mit dieser Rechtsfrage zu befassen.[61]

[Rz 59] Die Blockchain-Technologie könnte auch als öffentliches Register eingesetzt werden.[62] Ein Ersatz von zentralen Registern, wie dem Grundbuch, setzt eine Revision des geltenden Rechts voraus. Dies sollte jedoch erst in Betracht gezogen werden, wenn die Praxis in anderen Bereichen die Verlässlichkeit von Blockchains gezeigt hat und operationelle Risiken ausgeschlossen sind.

[Rz 60] Setzt sich die Blockchain-Technologie durch, werden sich, wie zurzeit bei Social Media, Fragen des Datenschutzes stellen. Das Blockchain-Prinzip der Unveränderbarkeit der Vergangenheit steht insbesondere im Widerspruch zum Recht auf Vergessen. Auch Anliegen des Konsumentenschutzes können ab diesem Zeitpunkt aktuell werden.

Dr. Jana Essebier ist Partnerin und Dominic A. Wyss ist Associate im Bereich des Finanzmarktrechts in der Kanzlei VISCHER AG, Zürich.

die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, S. 24 («Im Rahmen der Gespräche mit Expertinnen und Experten wurden auch andere Lösungen als die vorgesehenen Massnahmen erörtert, wie beispielsweise die Möglichkeit, Daten den Regeln für dingliche Verfügungs- und Nutzungsrechte zu unterstellen. Diese Lösungen wurden indessen in vielen Fällen als nicht umsetzbar beurteilt, da sie zu stark von den Entwicklungen auf internationaler Ebene abweichen (so sieht beispielsweise kein anderes europäisches Land Eigentumsrechte an Daten vor)»).

60 Vgl. in Bezug auf das Bereicherungsrecht Bärtschi/Meisser (Fn. 27), S. 144; zur Vollstreckung in Kryptowährungen vgl. Sébastien Gobat, Les monnaies virtuelles à l'épreuve de la LP – Questions choisies à l'exemple du bitcoin, AJP 2016, S. 1095 ff.

61 EFD FinTech (Fn. 3), S. 3, 15.

62 Geiling (Fn. 7), S. 31.