

## Versicherung 4.0

### Nutzung der Blockchain-Technologie und von Smart Contracts im Versicherungsbereich

#### Insurance 4.0

#### The use of blockchain technology and of Smart Contracts in the Insurance Sector

Frank Püttgen<sup>1</sup> · Markus Kaulartz<sup>2</sup>

Online publiziert: 7. September 2017  
© ERA 2017



**Zusammenfassung** Die Digitalisierungswelle hat auch die Versicherungswirtschaft voll erfasst. Der folgende Beitrag befasst sich mit der Blockchain-Technologie und sog. Smart Contracts sowie ihrer Eignung, den Versicherungssektor umzugestalten. Zunächst werden die Funktionsweise und der innovative Charakter der Blockchain-Technologie erläutert. Zudem wird anhand des Beispiels der „Blockchain Insurance Industry“-Initiative aufgezeigt, welches Interesse die Technologie bei Versicherern bereits geweckt hat. Das System der automatisierten Leistungsdurchführung von Smart Contracts wird näher beschrieben und vor dem Hintergrund des Vertragsschlusses rechtlich eingeordnet. Weiterhin werden die noch zu bewältigenden regulatorischen Herausforderungen näher definiert. Schließlich dienen Anwendungsbeispiele in der Versicherungswirtschaft dazu, das erlangte Verständnis für beide Technologien zu vertiefen.

**Schlüsselwörter** Digitalisierung des Versicherungssektors · InsurTech · Blockchain · Smart Contracts · B3i (Blockchain Insurance Industry Initiative)

**Abstract** The insurance industry has been hit by the digitalisation of business. This article deals with blockchain technology and smart contracts and their application within the insurance sector. First, the basic functioning and innovative character of

---

Für die Unterstützung bei der wissenschaftlichen Recherche bedanken sich die Autoren bei Frau Ref. jur. Claudia Willmer.

---

✉ Dr. M. Kaulartz  
[markus.kaulartz@cms-hs.com](mailto:markus.kaulartz@cms-hs.com)

Dr. F. Püttgen  
[frank.puettgen@cms-hs.com](mailto:frank.puettgen@cms-hs.com)

<sup>1</sup> CMS Hasche Sigle, Kranhaus 1, Im Zollhafen 18, 50678 Köln, Deutschland

<sup>2</sup> CMS Hasche Sigle, Nymphenburger Straße 12, 80335 München, Deutschland

the blockchain technology are explained. In addition, the insurers' interest which was aroused by the technology, is shown by means of the "Blockchain Insurance Industry Initiative". The method of automated performance of smart contracts is specified and legally classified. Furthermore, the regulatory challenges ahead are outlined. Finally, areas of application in the insurance industry serve to deepen the understanding of both technologies.

**Keywords** Digitalisation of the insurance industry · InsurTech · Blockchain · Smart contracts · B3i (Blockchain Insurance Industry Initiative)

## 1 Einleitung

Die Blockchain-Technologie ist in aller Munde und kaum eine Branche ohne erste Versuche, sie für eigene Unternehmenszwecke einzusetzen. Die einen sprechen von einem Hype, die anderen bescheinigen ihr einen disruptiven Charakter, als Fortführung einer Reihe bisheriger Innovationen, die die Welt verändert haben<sup>1</sup>: Großrechner (60er), Mikroprozessoren (70er), PC (80er), Internet (90er), Handys/Smartphones/Social Media (2000er und 2010er). Ihr ist eigen, dass Daten nicht mehr zentral, sondern verteilt gespeichert werden, dass zugleich aber sichergestellt wird, dass die bereits geschriebenen Daten nicht mehr geändert werden können. Einer zentralen Stelle in Form eines kontrollierenden Intermediärs – und das ist das wirklich Neue – braucht es hierfür nicht.

Auch in der Versicherungswirtschaft sind die mit der Blockchain-Technologie verbundenen Möglichkeiten nicht unerkannt geblieben. Dies zeigt sich unter anderem in der Gründung und fortschreitenden Entwicklung der „Blockchain Insurance Industry Initiative“ (B3i). Dieser weltweite Zusammenschluss von Versicherungsunternehmen und Rückversicherungsunternehmen, darunter beispielsweise Allianz und Munich Re, verfolgt das Ziel, das Potential der Blockchain-Technologie für die Rückversicherung und andere Anwendungen zu erforschen.

Eine weitere vielversprechende Technologie, deren Leistungsvermögen es für die Versicherungswirtschaft noch zu erforschen gilt, stellen sogenannte „Smart Contracts“ dar. Bei Smart Contracts handelt es sich um Software, die vorprogrammierte Aktionen bei Eintritt einer bestimmten Bedingung automatisch selbst ausführt. Ihr Potential erscheint insbesondere in der Verknüpfung mit der Blockchain-Technologie als bahnbrechend.

Der Beitrag geht auf die Technik der Blockchain ein, erläutert Smart Contracts vor dem Hintergrund von Anwendungsfällen in der Versicherungswirtschaft und schließt mit einem Ausblick auf regulatorische Rahmenbedingungen.

## 2 Das Besondere an der Blockchain-Technologie

Eine Blockchain ist ein sogenannter „distributed ledger“, also eine verteilt gespeicherte Datenbank.<sup>2</sup> Diese Datenbank wird in identischer Form auf miteinander kom-

<sup>1</sup> Vgl. Blocher [1], S. 612.

<sup>2</sup> Ausführlich zur Technik der Blockchain vgl. Kaulartz [7], p. 474 ff.; Sorgel/Krohn-Grimberghe [15], S. 479 ff.; Narayanan/Bonneau/Felten/Miller/Goldfeder [12], passim.

munizierenden Rechnern in einem Peer-to-Peer-Netzwerk gespeichert. Alle jemals getätigten Änderungen an dieser Datenbank können jederzeit nachvollzogen werden, was darin begründet liegt, dass keine Daten aus der Blockchain gelöscht, sondern nur in sie hineingeschrieben werden können. Das hat damit zu tun, dass neue Daten als Blöcke an die bestehenden Datenblöcke angehängt werden – daher der Name „Blockchain“. Da Blöcke nur valide sind, wenn die Blöcke vor ihnen nicht verändert wurden, würde jede Manipulation sofort auffallen.

Das Besondere an der Technologie ist, dass sie auf einen kontrollierenden, vertrauenswürdigen Intermediär verzichtet: Nicht eine solche zentrale Stelle verantwortet die Integrität der Datenbank, sondern eine Mehrheit der teilnehmenden Rechner.<sup>3</sup> Die Rede ist von einem „consensus“-Mechanismus. Damit bricht sie mit dem bislang vorherrschenden Client-Server-Prinzip, bei welchem der Server in der Mitte steht und eine Vielzahl von Clients bedient. Bei einer Blockchain sind alle Teilnehmer gleichberechtigt und stehen in ihrer Wertigkeit auf derselben Stufe: Jeder Teilnehmer speichert die vollständige Blockchain.<sup>4</sup>

Als Vergleich stelle man sich einen Kurs vor, in welchem bisher der Kursleiter die Anwesenheitsliste geführt hat. Dem Kursleiter und der von ihm erstellten Anwesenheitsliste muss vertraut werden, um im Nachhinein die Anwesenheit der Kursteilnehmer festzustellen. Die Blockchain-Technologie geht einen anderen Weg: Um im Bild zu bleiben, führt jeder Kursteilnehmer eine eigene Anwesenheitsliste und hält sie zudem noch in die Höhe, um sie von allen anderen Kursteilnehmern kontrollieren und bestätigen zu lassen. Damit die Anwesenheitsliste auch geführt wird und sich nicht jeder darauf verlässt, dass andere dies übernehmen, erhalten die Kursteilnehmer Anreize in Form von Belohnungen. Im Falle der Blockchain sind dies geldwerte virtuelle Währungen.

Das bekannteste und zugleich auch erste Beispiel einer Blockchain-Implementierung und solcher virtueller Währungen ist Bitcoin. Bitcoins gehen auf ihren unbekannten Schöpfer Satoshi Nakamoto zurück<sup>5</sup> und haben in den vergangenen Jahren immens an Wert gewonnen.<sup>6</sup> Will man sich die Vorzüge einer Blockchain am Beispiel von Bitcoins bildlich vorstellen, so ist das Bezahlen von Bitcoins mit dem Bezahlen mit einer Geldmünze vergleichbar. Wir akzeptieren eine Geldmünze, weil wir sie als echt zu erkennen meinen, und ihr zugleich einen bestimmten Wert attestieren. Einmal ausgegeben, ist die Münze nicht mehr in unserer Verfügungsgewalt. Auch Bitcoins können nicht mehrmals, sondern nur einmal ausgegeben werden. Durch die Bitcoins immanente elektronische Signatur wird zudem die Authentizität sichergestellt.<sup>7</sup>

<sup>3</sup>So jedenfalls im Falle des Proof-of-Work-Verfahrens.

<sup>4</sup>Im Detail gibt es Abstufungen, die hier nicht näher beleuchtet werden sollen.

<sup>5</sup>Vgl. Nakamoto [11], passim (zuletzt abgerufen am 25.7.2017).

<sup>6</sup>Vgl. etwa <https://blockchain.info/charts> (zuletzt abgerufen am 25.7.2017).

<sup>7</sup>Aktuelle Entwicklung von Bitcoins: Dienstag, den 1.8.2017 wurde das Bitcoinsystem in die bisherige Bitcoinblockchain und eine neue Bitcoin-Cash-Blockchain aufgespalten. Die Spaltung von Bitcoin beruht auf einem Streit der Bitcoin-Anhänger darüber, in welchem Umfang die Megabytegröße eines einzelnen Blocks der Blockchain erhöht werden soll. Während die Blöcke der bisherigen Blockchain in den nächsten drei Monaten auf mindestens zwei Megabyte erhöht werden soll, liegt die Größe der Bitcoin Cash-Blocks bei acht Megabyte.

Ohne die Blockchain-Technologie ist ein digitales Bezahlen stets auf einen Intermediär angewiesen (etwa eine Bank), der sicherstellt, dass das digitale Geld nicht zweimal ausgegeben werden kann, so wie man etwa ein PDF-Dokument auch an mehrere Empfänger in identischer Form verschicken kann, ohne dass die einzelnen Empfänger wissen, dass dieselbe Datei kopiert und mehrmals verwendet wird. Die Blockchain-Technologie setzt hier an und schafft die Voraussetzungen für virtuelle Währungen.

### 3 Charakteristika von Blockchains

Die technischen Hintergründe einer Blockchain zu durchsteigen ist nicht einfach und erfordert viel technischen Sachverstand.<sup>8</sup> Um Anwendungsbereiche zu verstehen und um an der Diskussion zum Thema teilzunehmen, ist vertieftes Hintergrundwissen indes nicht notwendig. Hierfür genügt es zu Beginn schon, die wesentlichen Charakteristika einer Blockchain zu verstehen:

Eine Blockchain ist zunächst einmal transparent,<sup>9</sup> denn die verteilt gespeicherte Datenbank mitsamt allen getätigten Änderungen kann von allen Berechtigten eingesehen werden.

Sie ist außerdem praktisch nicht manipulierbar, da sie auf kryptographischen Verfahren beruht und Transaktionen nur von jenen Personen durchgeführt werden können, die über den zu den jeweiligen Transaktionen passenden privaten Schlüssel verfügen.

Die Blockchain-Technologie ist ferner nicht bestechlich, da sie auf Grund der kryptographischen Eigenschaft vorgegebenen Regeln folgt, die nicht abänderbar sind. Zudem hat sie eine hohe Ausfallsicherheit und Widerstandsfähigkeit, da alle Daten verteilt gespeichert werden und der Datenverlust auf einem einzelnen Rechner durch dieselben Datenbestände auf anderen Rechnern aufgefangen wird.

Schließlich ist die verteilt gespeicherte Datenbank integer, da einzelne Datensätze nicht geändert werden können.

Diese Eigenschaften stehen im Gegensatz zu einer zentralen, Vertrauen schaffenden Stelle, die stets der "single point of failure" und Ziel möglicher Angriffe ist. Gedacht sei etwa an einen Server, der ausfällt und damit einen Online-Dienst zum Erliegen bringt.

### 4 Blockchain Insurance Industry Initiative (B3i)

Das Potential der Blockchain-Technologie hat auch der Versicherungssektor für sich erkannt. Dort ist das Interesse an InsurTech in den letzten Jahren rasant angestiegen. Es ist eine deutliche Zunahme an Investitionen in Start-Ups, die eigene Forschung von Versicherungsunternehmen oder Kooperationen mit anderen Unternehmen erkennbar.<sup>10</sup> Ein Beispiel für diese Entwicklung bildet die „Blockchain Insurance In-

<sup>8</sup>Einführend etwa Blocher [1], S. 612; Kaulartz [7], S. 474 ff.

<sup>9</sup>Vgl. Guggenberger [4], S. 49; Peschl/Böhme [13], S. 93 ff.

<sup>10</sup>Vgl. Blockchain in insurance – opportunity or threat, <http://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat> (zuletzt abgerufen am 27.7.2017).

dustry Initiative“ (B3i), welche im Oktober 2016 gegründet wurde. Die fünf Gründungsmitglieder Aegon, Allianz, Munich Re, Swiss Re und Zurich haben sich mit dem Ziel zusammengeschlossen, in gemeinsamer Kooperation einen besseren Einblick in die Anwendungsmöglichkeiten der Blockchain-Technologie im Versicherungsmarkt zu erforschen.<sup>11</sup> Bereits im Juni 2017 begrüßte der Zusammenschluss zehn weitere Erst- und Rückversicherer<sup>12</sup> als neue Mitglieder.<sup>13</sup> Damit gehören der B3i mittlerweile Mitglieder aus Asien, Europa und dem amerikanischen Kontinent an und der ursprünglich mitteleuropäische Zusammenschluss hat sich zu einer weltweiten Initiative entwickelt.

Ein Schwerpunkt der Initiative liegt in der Erforschung, ob die Blockchain-Technologie dazu genutzt werden kann, den Datenaustausch zwischen Erst- und Rückversicherer effizienter zu gestalten<sup>14</sup> und somit mittels der Distributed-Ledger-Technologie die Retrozession innerhalb der Gruppe der Mitglieder zu vereinfachen. Die B3i versucht in diesem Sinne Standards und Verfahrensweisen für eine branchenweite Nutzung zu entwickeln und daraus Effizienzsteigerungen für die Versicherungswirtschaft zu generieren.<sup>15</sup> Neben der gemeinsamen Forschung soll die Initiative jedoch auch als Plattform zum Austausch von Erfahrungen mit Blockchain- und anderen Technologien und weiteren Pilotprojekten oder Forschungsergebnissen dienen.<sup>16</sup>

## 5 Smart Contracts – automatisierte Leistungsdurchführungen

### 5.1 Erläuterung

Von der Blockchain-Technologie zu trennen sind sogenannte „Smart Contracts“. Dabei handelt es sich schlicht um Software, die eine vertraglich vereinbarte Leistung durchführt.<sup>17</sup> Das meint nicht eine Software, mit welcher ein Programmierer das vertraglich geschuldete Programm schreibt. Gemeint ist tatsächlich eine Software, welche die Hauptleistung eines Vertrages erbringt, ohne dass es einer weiteren menschlichen Komponente bedarf. Dies verdeutlicht bereits, dass Smart Contracts überall dort zum Einsatz kommen können, wo eine digital zugängliche Leistung geschuldet wird,

<sup>11</sup>Vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2016/2016-10-19-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

<sup>12</sup>XL Catlin, Hannover Rück, Achmea, Generali, SCOR, Ageas, Sampo Japan, RGAs, Tokio Marine, Liberty Mutual.

<sup>13</sup>Vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2017/2017-02-06-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

<sup>14</sup>Vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2017/2017-02-06-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

<sup>15</sup>Vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2016/2016-10-19-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

<sup>16</sup>Vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2016/2016-10-19-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

<sup>17</sup>Vgl. ausführlich zu Smart Contracts Kaulartz/Heckmann [6], S. 618 ff.; ferner Jacobs/Lange-Hausstein [5], S. 10 ff.; Djazayeri [3], Anm. 1.

also etwa bei der Bezahlung mit Geld, dem Versand einer E-Mail oder dem Speichern oder Verändern von Datensätzen.

Auch wenn der Name zunächst Gegenteiliges vermuten lässt, handelt es sich bei Smart Contracts also gerade nicht um Verträge, sondern lediglich um die Durchführung eines Realakts.<sup>18</sup> Die Verbindung mit einem Vertrag erfolgt vielmehr über die Verknüpfung zwischen Leistungsdurchführung und Rechtsgrund. Im Vertrag wird also etwa vereinbart, dass mittels Smart Contract erfüllt werden soll. Fehler in der Programmierung von Smart Contracts lassen den Erfüllungsanspruch unberührt oder führen zu einer Nacherfüllung oder sonstigen Gewährleistungsrechten.

Für den Bereich von Versicherungsverträgen ergibt sich etwa folgendes Anwendungsbeispiel von Smart Contracts: So kann im Rahmen einer Flugausfallversicherung vereinbart werden, dass die Vertragsleistung mittels eines Smart Contracts erbracht werden soll. Bei einem anhand der Flugdatenbank registrierten Ausfall des versicherten Fluges erbringt der Smart Contract sodann automatisch die Auszahlung der entsprechenden Versicherungssumme an den Versicherungsnehmer.

Wie das Beispiel zeigt, orientieren sich Smart Contracts im Wesentlichen an der Fähigkeit von Computern, logische Bedingungen abzarbeiten. In dem Programmcode eines Smart Contracts werden für das Eintreten bestimmter Bedingungen bestimmte Folgen nach dem Schema „Wenn dies, dann das“ definiert. Bei Bedingungseintritt löst der Smart Contract sodann automatisch die zuvor festgelegte Folge aus. Auf rechtlicher Ebene entspricht dies der Erbringung der vertraglich vereinbarten Leistung. Da die Leistung bzw. Vertragserfüllung von einer konkreten Bedingung abhängig ist, muss der Eintritt oder das Ausbleiben dieser Bedingung digital überprüfbar sein. Damit Ereignisse, die in der realen Welt eintreten, digital erfassbar sind, bedarf es einer Verknüpfung der analogen mit der digitalen Welt. Diese „Übersetzung“ realer Ereignisse erfolgt mittels „IT-Schnittstellen“. Die als „oracles“ bezeichneten Schnittstellen ermöglichen eine Interaktion des Smart Contracts mit der realen Welt.<sup>19</sup> So würde in dem oben genannten Beispiel das reale Ereignis des Flugausfalls erfasst, indem der Smart Contract via Internet mit einer Flugdatenbank verbunden ist und den Ausfall digital erfasst.

## 5.2 Smart Contracts und Vertragsschluss

Natürlich ist es nicht ausgeschlossen, dass die Durchführung eines Smart Contracts mit einem Vertragsschluss zusammenfällt. Vergleichbar zum Bargeschäft des täglichen Lebens könnten die Übergabe von Ware und Geld also zugleich als Angebot und Annahme im Sinne der §§ 145 ff. BGB gesehen werden. Der Inhalt des Vertrages ergibt sich nach dem objektiven Empfängerhorizont, §§ 133, 157 BGB, hier also etwa aus den Inhalten der Webseite, über welche ein Smart Contract abgeschlossen wird. Fehlt es an einer solchen, stellt sich die bislang wenig diskutierte Frage, ob auch der Code des Smart Contracts zur Bestimmung des Vertragsinhalts herangezogen werden könnte.<sup>20</sup> Solange aus Sicht eines objektiven Empfängers von einer

<sup>18</sup>Ausführlich hierzu Kaulartz/Heckmann [6], S. 618 ff.

<sup>19</sup>Kaulartz/Heckmann [6], S. 618 ff.

<sup>20</sup>Näher hierzu Kaulartz [8], S. 201 ff. mwN; vgl. auch Schrey/Thalhofer [14], S. 1431.

wirksamen Willenserklärung unter Vorliegen insbesondere des Erklärungsbewusstseins ausgegangen werden kann, scheint dies durchaus nicht fernliegend. Schließlich schreibt das BGB und die aus Art. 2 Abs. 1 GG zu folgernde Vertragsfreiheit nicht vor, in welcher Sprache ein Vertrag abzufassen ist. Im Falle von AGB – wenn also der Smart Contract, wie meist, für eine Vielzahl von Verträgen vorformuliert zum Einsatz kommt – mag man zu einer Unwirksamkeit kommen. Vorzugswürdig erscheint es aber, die AGB-Kontrolle bei einem Formularvertrag, bei welchem die Einbeziehung von AGB keine Rolle spielt, als reine Inhaltskontrolle zu verstehen und das Problem auf der Ebene der Willenserklärung zu suchen.<sup>21</sup> Schließlich ist die Hürde, die es zu nehmen gilt, damit der Verkehr von einer wirksamen Willenserklärung ausgeht, recht hoch.

Nicht vergessen werden darf bei dieser Diskussion aber ihre Praxisrelevanz. Da Smart Contracts nur zur Leistungsdurchführung eingesetzt werden, lässt sich mit ihnen eigentlich nur ein kleiner Teil eines Vertrages abbilden. Kein Raum ist für Nebenpflichten, Haftungs- und Gewährleistungsklauseln oder Kündigungsvorschriften etc.<sup>22</sup> Es bietet sich daher an, Smart Contracts nur dort zum Einsatz zu bringen, wo sie ihre Stärke ausspielen, nämlich bei der Vertragserfüllung.<sup>23</sup> Alles andere sollte separat geregelt werden, etwa in einem AGB-Dokument, das bei Abschluss des Smart Contracts vereinbart wird.

### 5.3 Herausforderungen bei der Entwicklung von Smart Contracts

Im Gegensatz zu anderer Software kommt Smart Contracts die Eigenschaft zu, zur Vertragserfüllung genutzt zu werden. Dies verlangt von ihnen, nicht von den Verträgen, die sie erfüllen sollen, abzuweichen. In solchen Fällen nämlich müssten Gewährleistungsrechte ausgeübt werden, was mittels Smart Contracts nur umständlich möglich ist.

Wichtiger ist es daher, eine Code-Compliance des Smart Contract Code zu erreichen. Als neues Betätigungsfeld für Juristen müssten diese zusammen mit Entwicklern darüber Einigkeit herstellen, wie Vertragsklauseln und Gesetze in Codes umzusetzen sind. Die größte Schwierigkeit liegt dabei in unbestimmten Rechtsbegriffen, die von Software naturgemäß nur schwer interpretiert werden können. Daneben ist zu bedenken, dass ein Rechtsverhältnis aus mehr besteht als ein paar wenigen Vertragsklauseln: Alleine das BGB hält zahlreiche Vorschriften bereit, die Anwendung finden oder in bestimmten Fällen Anwendung finden können. Das BGB indes in einen Smart Contract hinein zu programmieren, erscheint wenig sinnvoll. Hier braucht es vielmehr vernünftige Governance- und Schiedsgerichtsschnittstellen,<sup>24</sup> um auf Erfüllungsebene adäquat reagieren zu können.

---

<sup>21</sup>Vgl. Kaulartz/Heckmann [6], S. 618, 622.

<sup>22</sup>Natürlich könnten in den Code des Smart Contracts sonstige Klauseln auch als Kommentare hinterlegt werden, was einen Medienbruch verhindert. Auch dies mag für die Praxis jedoch nicht recht überzeugen.

<sup>23</sup>An dieser Stelle käme allerdings auch eine dingliche Einigung in Betracht.

<sup>24</sup>Vgl. Kaulartz [9].

## 6 Vorteile und Nachteile der Blockchain-Technologie und von Smart Contracts

Die Versprechen der Blockchain-Technologie und darauf aufbauend von Smart Contracts sind aussichtsreich: Fälschungssichere Transaktionen, dezentrale, transparente Speicher, Integrität von Daten. Hinzu kommt der Verzicht auf einen Intermediär wie etwa eine Bank, einen E-Mail-Provider oder einen Online-Dienst: Die Blockchain-Technologie steht für sogenannten „trustless trust“. Damit wird zum Ausdruck gebracht, dass niemandem, insbesondere keinem Intermediär, Vertrauen geschenkt werden muss. Das Vertrauen in die Technologie, insbesondere die eingesetzte Kryptographie, genügt, um Geschäfte durchzuführen.<sup>25</sup>

Natürlich mag hier eingewendet werden, dass Verschlüsselungen grundsätzlich „geknackt“ bzw. „gehackt“ werden könnten, was insbesondere im künftigen Zeitalter der Quantencomputer nicht ausgeschlossen sein mag. Dieses Problem stellt sich jedoch nicht nur bei Blockchains, sondern bei jedweder verschlüsselter Kommunikation im Internet. Die Blockchain-Technologie hebt sich allerdings dadurch hervor, dass durch geschickte Gestaltung der in einer Reihe verbundener Blöcke der Rechenaufwand zur Manipulation derselben im Moment dermaßen hoch wäre, dass im Vergleich zu sonstigen Technologien trotzdem von einer signifikanten Steigerung von Sicherheit gesprochen werden kann. Durch die Verwendung von Hashwerten ist es überdies ausgeschlossen, bei einem Angriff ganze Datenbanken mit Klartextinformationen abziehen. Denn Hashwerte enthalten lediglich eine Art Fingerabdruck von Rohdaten, vergleichbar der Quersumme einer großen Zahl. So, wie von der Quersumme nicht auf die Zahl geschlossen werden kann, können auch nicht die Rohdaten aus einem Hashwert wiederhergestellt werden.

Daneben stellen sich derzeit weitere, zahlreiche Herausforderungen<sup>26</sup>: Eine Blockchain im Masseneinsatz sollte skalierbar und schnell sein, was heute meist noch nicht der Fall ist. Auch sollte Nachhaltigkeit eine Rolle spielen, was sich mit dem teils hohen Energieverbrauch von Blockchains kaum vereinbaren lässt. Da Transaktionen in der Blockchain nachvollziehbar und transparent gespeichert werden, bedarf es Lösungen zur Durchsetzung des unter Umständen einschlägigen Rechts auf Vergessen,<sup>27</sup> außerdem müssen irrtümliche Fehlbuchungen korrigiert werden können. Hierfür bedarf es Governance- und Arbitration-Lösungen, welche die Vorteile von Blockchains nicht zunichte machen. Schließlich ist es in jedem Einzelfall wichtig zu bestimmen, welche Daten datenschutzkonform in der Blockchain gespeichert werden oder wo eine Abwägung mit der Sensibilität der Information dazu führt, auf eine Speicherung zu verzichten. Ein weiteres Thema betrifft die Standardisierung, welche die Migration von Datenbeständen heute praktisch unmöglich macht.

Die Akzeptanz einer Blockchain steht und fällt mit der Einfachheit der Bedienung (Nutzerfreundlichkeit). Da schon die qualifizierte elektronische Signatur des Personalausweises wegen des hohen Aufwands ihrer Einrichtung kaum zum Einsatz kommt,<sup>28</sup> sind die Anforderungen an die Implementierung einer Blockchain nicht

<sup>25</sup> Insofern ist die Bezeichnung „trustless trust“ missverständlich.

<sup>26</sup> Vgl. ferner *McLean/Deane-Johns* [10], S. 97, 100 f.

<sup>27</sup> Vgl. *Böhmel/Pesch* [2], S. 473, 480.

<sup>28</sup> Vgl. etwa *Stiemerling* [16] (zuletzt abgerufen am 25.7.2017).



zu unterschätzen. Hierbei ist zudem zu berücksichtigen, dass der Einsatz von Software als Schnittstelle zur Blockchain naturgemäß wieder fehleranfällig ist, da hier die kryptographischen Vorzüge der Blockchain-Technologie nicht zum Tragen kommen.<sup>29</sup> Schneidet also etwa ein Angreifer den privaten Schlüssel eines Nutzers mit Hilfe eines Trojaners auf dessen Rechner mit, verfügt er über die Befähigung zur Unterschrift im Namen des besagten Nutzers. Ein Risiko, das vor dem Hintergrund der Rechtswirkungen von Blockchain-Transaktionen auf wenig Gegenliebe stoßen dürfte. Die Lösung sollte darin liegen, die Blockchain zumindest in einem ersten Schritt nur als Hintergrundtechnologie zu verwenden. So käme in Betracht, dass zum Beispiel Grundbuchämter eine Blockchain zur Verwaltung von Rechten an Grundstücken einsetzen, was noch lange nicht bedeutet, dass Käufer und Verkäufer von Immobilien einen Kaufvertrag nur mittels eines eigenen Zugangs zu einer Blockchain erfüllen können.

Auch wenn die Blockchain zu höherer Sicherheit und zu Kostensenkungen führen kann, so darf nicht übersehen werden, dass die Technologie heute noch in den Kinderschuhen steckt. Vergleichbar mit der Entstehung des Internets, das mit seiner Client-Server-Struktur zentral und gerade nicht dezentral aufgebaut ist, wird es noch eines Reifeprozesses brauchen, bis kritische Dienste einzig und allein auf einer Blockchain laufen.

## 7 Anwendungsbereiche in der Versicherungswirtschaft

Während sich Start-Ups und Investoren in der Vergangenheit zunächst auf den Zahlungsverkehr und das Bankgeschäft fokussiert haben, stehen nun auch zunehmend Versicherungslösungen im Blickfeld der Entwicklung. Versicherungsunternehmen investieren in InsurTech Start-Ups oder ergreifen Eigeninitiative, um die Anwendungsmöglichkeiten und das Potential der Blockchain-Technologie und Smart Contracts zu erforschen.

Wie dargestellt, führen Smart Contracts vorprogrammierte Aktionen automatisch aus, sobald eine oder mehrere vereinbarte und im Vertragsprogrammcode vorformulierte Bedingung(en) eingetreten ist oder sind. Aufgrund dieser Struktur können durch den Einsatz von Smart Contracts wesentliche Schlüsselprozesse des Versicherungsvorgangs automatisiert werden. Ergänzend hierzu kann die Blockchain als dezentrale Datenbank diejenige Sicherheit gewährleisten, die für die Abwicklung von Transaktionen zwischen Parteien, auch unter Einbeziehung verschiedener Unbekannter, erforderlich ist.<sup>30</sup> Die Anwendungsbereiche beider Technologien im Rahmen der Versicherungswirtschaft sind vielfältig.

Ein potientieller Einsatzszenario ist etwa die automatische Anpassung der Versicherungsprämie an das Verhalten des Versicherungsnehmers. Durch eine Verknüpfung der Technologien mit dem Internet der Dinge ist dies beispielsweise für die

<sup>29</sup>Vergleichbar ist dies etwa mit den Angriffen auf Anbieter von Bitcoin-Wallets. Diese Anbieter speicherten die privaten Schlüssel der Bitcoin-Nutzer. Da Angreifer sich hierauf vereinzelt Zugriff verschaffen konnten, konnten sie auch über die entsprechenden Bitcoins verfügen.

<sup>30</sup>Vgl. Jacobs/Lange-Hausstein [5], S. 10–15.

Kfz-Versicherung möglich. Der PKW kann über telemetrische Sensoren den Fahrstil des Versicherungsnehmers aufzeichnen. Über die Konnektivität internetbasierter Objekte<sup>31</sup> können die erkannten und aufgezeichneten Daten des Fahrstils sodann via Internet an den Versicherer weitergeleitet werden. Der vorprogrammierte Smart Contract kann die empfangenen Daten verarbeiten und bei einem risikoreichen oder risikoarmen Fahrstil des Versicherungsnehmers die Versicherungsprämie automatisch an diesen anpassen.<sup>32</sup> Eine „personalisierte“ Prämienanpassung ist ebenso bei der Versicherung von Schiffen denkbar. Über GPS kann der Standort des Transportmittels an den Versicherer mitgeteilt werden. Befindet sich das Schiff in einer Gefahrenzone, wie etwa in einem Gebiet mit hohem Risiko von Piraterie (etwa an der Küste vor Somalia am Horn von Afrika), kann die Versicherungsprämie automatisch erhöht werden.

Auch bei der Abwicklung des Zahlungsverkehrs in der Versicherungsbranche können die genannten Technologien von Nutzen sein. So könnte beispielsweise die Auszahlung der Versicherungssumme, sobald das registrierte Schadenereignis verifiziert wurde, automatisch durch den Smart Contract initiiert werden. Bei einem digital verifizierbaren Schadenereignis, wie zum Beispiel einem durch Sensoren erkannten und aufgrund des Internets der Dinge an den Versicherer mitgeteilten Schaden am Auto, wären theoretisch sogar Echtzeitzahlungen mit dem Eintritt des Schadenereignisses möglich.

Die Überprüfung von Daten und ihre Anpassung an sich ändernde Umstände, die Bestätigung von Schadenfällen sowie die Abwicklung des Zahlungsverkehrs, wie sie in den Beispielen aufgezeigt wurden, sind jedoch nicht die einzigen Einsatzmöglichkeiten von Blockchain und Smart Contracts. Ebenso könnten die Kontrolle von Prozessabläufen, die Administration des Versicherungsschutzes oder die Beglaubigung und Verifizierung von Identitäten, Vorgängen und Dokumenten durch die beiden Technologien übernommen werden, ohne dass eine weitergehende Überprüfung oder manuelle Verwaltung des Schadenfalls zu erfolgen hätte. Mittels Blockchain und Smart Contracts können die Vorgänge der Schadenbearbeitung, -prüfung und -feststellung vereinfacht und beschleunigt und damit die Bearbeitungsdauer von Schadenfällen insgesamt verkürzt werden. Zudem bewirkt die Prozessautomatisierung, dass die Fehlerquelle „menschliches Fehlverhalten“ bei Versicherungsvorgängen verringert bzw. sogar eliminiert wird. Insofern können durch die Verwendung von Smart Contracts im Versicherungssektor Kosten und Zeit eingespart werden.

Derartige Einsatzszenarien bleiben jedoch nicht fiktiv. Bereits heute gibt es Unternehmen, die innovative Versicherungslösungen unter Anwendung von Smart Contracts oder der Blockchain Technologie anbieten. Beispiele dafür bilden die Start-Ups InsurETH<sup>33</sup> und Dynamis.<sup>34</sup>

InsurETH ist eine Flugverspätungsversicherung, bei welcher die Versicherungssumme für verspätete bzw. gestrichene Flüge mittels eines Smart Contracts automatisch ausgezahlt wird. Die Einzahlung der Versicherungsprämie und die Auszahlung der Versicherungssumme erfolgen in der virtuellen Währung „Ether“, denn

<sup>31</sup> Objekte, die Daten aus dem Internet senden und empfangen können.

<sup>32</sup> Vgl. *Djazayeri* [3], Anm. 1.

<sup>33</sup> Vgl. <http://insureth.mkvd.net> (zuletzt abgerufen am 26.7.2017).

<sup>34</sup> <http://dynamisapp.com/vision.html>.

die InsurETH-Versicherung setzt auf der öffentlichen Blockchain „Ethereum“<sup>35</sup> auf. Das Start-Up nutzt die historischen Flugverspätungs- und Flugausfalldaten der globalen Flugdatenbank. Anhand der Flugdaten der letzten drei Monate wird die Flugverspätungs- und Flugausfallwahrscheinlichkeit ermittelt und die potentielle Auszahlungssumme an das geschätzte Ergebnis angepasst. Übermittelt die Datenquelle der globalen Flugdatenbank die Verspätung oder Streichung des versicherten Fluges, so bewirkt der Smart Contract automatisch die Auszahlung der Versicherungssumme an den Versicherungsnehmer.

Weiterhin bietet das Start-Up Dynamis eine private Arbeitslosenversicherung an, welche auf dem Prinzip der Gegenseitigkeit basiert. Die Versicherungsnehmer sind zugleich auch Teilhaber der Versicherung und zudem obliegt ihnen die Schadenbearbeitung. Das Schadenmanagement erfolgt über soziale Netzwerke wie LinkedIn. Diese dienen zum einen dazu, die Identität der Versicherungsnehmer zu überprüfen, und zum anderen den Arbeits- bzw. Arbeitslosenstatus zu verifizieren. Daher ist es erforderlich, dass alle Mitglieder der Versicherung dem gleichen sozialen Netzwerk angehören. Ebenfalls die öffentliche Blockchain „Ethereum“ nutzend, erhält der Versicherungsnehmer, soweit seine Arbeitslosigkeit von der Mehrzahl der anderen Versicherungsnehmer verifiziert wurde, eine monatliche Auszahlung in der Kryptowährung „ether“. Das System der gegenseitigen Überprüfung und Anerkennung macht Intermediäre entbehrlich.

## 8 Regulierung

Die wirtschaftliche Betätigung im Finanzsektor ist auf nationaler sowie auf europäischer Ebene durch umfassende aufsichtsrechtliche Bestimmungen geregelt. Diese regulatorischen Vorgaben bilden gemeinsam mit der Verwaltungspraxis der maßgeblichen Aufsichtsbehörden<sup>36</sup> auch für den Versicherungssektor die Rahmenbedingungen. Smart Contracts erlangen regulatorische Relevanz, wenn Personen oder Unternehmen unter Rückgriff auf eine Blockchain in den Finanzbereich vordringen. In Bezug auf die Verwendung von Smart Contracts bestehen allerdings weiterhin viele regulatorische Unsicherheiten und ungeklärte Fragen.

Auf deutscher Ebene sind bisher keine expliziten, aufsichtsrechtlichen Verlautbarungen im Hinblick auf die Anwendung von Smart Contracts getroffen worden. Es wurden lediglich Äußerungen bezüglich „virtueller Währungen“ gemacht. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat beispielsweise zu der aufsichtsrechtlichen Bewertung von „Bitcoins“ Stellung genommen. Die BaFin benannte die virtuelle Währung „Bitcoins“ als Rechnungseinheit und folglich als Finanzinstrument im Sinne des § 1 XI Nr. 7 KWG.<sup>37</sup>

Ebenso bestehen auf europäischer Ebene noch keine Ansätze für eine einheitliche regulatorische Behandlung von Smart Contracts. Allerdings befassen sich auch

<sup>35</sup> Vgl. <https://www.etherum.org> (zuletzt abgerufen am 26.7.2017).

<sup>36</sup> Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), European Securities and Market Authority (ESMA).

<sup>37</sup> Vgl. [https://www.bafin.de/ShareDocs/Veroeffentlichungen/DE/Merkblatt/mb\\_111220\\_finanzinstrumente.html](https://www.bafin.de/ShareDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html) (zuletzt abgerufen am 26.7.2017).

der europäische Gesetzgeber und die europäischen Aufsichtsbehörden mit der allgemeinen Thematik „virtueller Währungen“. Die Diskussion aufsichtsrechtlicher Regelungen in diesem Sinne begann mit einem Berichtsentwurf des Ausschusses für Wirtschaft und Währung (ECON) im Februar 2016<sup>38</sup> und dem Aktionsplan gegen Terrorismusfinanzierung der Kommission,<sup>39</sup> ebenfalls aus demselben Monat. Beide Dokumente setzen sich unter anderem mit der Bedeutung virtueller Währungen und der „Distributed-Ledger-Technologie“ sowie ihren Risiken auseinander. Die benannten Risiken führten schließlich zu dem Vorschlag des Europäischen Parlaments und des Rates vom 5. Juli 2016, die Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorfinanzierung zu ändern.<sup>40</sup> Nach dem Änderungsvorschlag soll der sachliche Anwendungsbereich der Richtlinie auf Plattformen, auf denen virtuelle Währungen getauscht werden können, und auf Anbieter von elektronischen Geldbörsen erweitert werden.<sup>41</sup> Insgesamt sollen die zuständigen Aufsichtsbehörden durch die Neuregelung der Richtlinie in die Lage versetzt werden, die Verwendung virtueller Währungen überwachen zu können.<sup>42</sup> Mit Beginn des Gesetzgebungsprozesses haben sich der parlamentarische Ausschuss für Wirtschaft und Währung (ECON) sowie der parlamentarische Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) für die Ausarbeitung der Änderungsrichtlinie für zuständig erklärt. Am 7. November 2016 wurde ein erster Richtlinienentwurf vorgestellt.<sup>43</sup> Unter Zustimmung des Plenums des Europäischen Parlaments beteiligt sich der Gemeinsame Ausschuss der europäischen Aufsichtsbehörden ebenfalls an den interinstitutionellen Verhandlungen zur Ausarbeitung einer endgültigen Fassung der Änderungsrichtlinie.<sup>44</sup> Bis zum jetzigen Zeitpunkt wurde das Gesetzgebungsverfahren jedoch noch nicht beendet.

## 9 Ausblick

Die Geschichte des Geldes reicht weit zurück. Zahlungsmittel wurden immer wieder an sich ändernde Umstände angepasst. Das ursprüngliche Natural- oder Warengeld wurde im Hinblick auf Zählbarkeit, Lagerfähigkeit und Transportierbarkeit zunächst

<sup>38</sup> Vgl. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPAL%2BPE-575.277%2B01%2BDOC%2BPDF%2BV0%2F%2FEN> (zuletzt abgerufen am 26.7.2017).

<sup>39</sup> Vgl. <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1455113825366&uri=CELEX:52016DC0050> (zuletzt abgerufen am 26.7.2017).

<sup>40</sup> Vgl. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52016PC0450> (zuletzt abgerufen am 26.7.2017).

<sup>41</sup> Vgl. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52016PC0450> (zuletzt abgerufen am 26.7.2017).

<sup>42</sup> Vgl. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52016PC0450> (zuletzt abgerufen am 26.7.2017).

<sup>43</sup> Vgl. [http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-\(aml\)](http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)) (zuletzt abgerufen am 26.7.2017).

<sup>44</sup> Vgl. [http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-\(aml\)](http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)) (zuletzt abgerufen am 26.7.2017).

durch Münzgeld und später durch Papiergeld ersetzt. Heute existiert Internetbankhandel, und Kredit- sowie Debitkarten bilden das Standardzahlungsmittel. Die Nutzung digitaler Währungen unter Anwendung der Blockchain-Technologie und die Automatisierung der Vertragserfüllung durch Smart Contracts sind der nächste große Schritt dieser Entwicklung.

Das Potential, welches beide Technologien dabei gerade auch für die Versicherungswirtschaft mit sich bringen, ist nicht zu übersehen. Für Versicherungsunternehmen ist es deshalb wichtig, bereits jetzt die Anwendungsmöglichkeiten von Smart Contracts und Blockchain-Technologie sowie deren Auswirkungen auf die Versicherungsbranche zu prüfen, um Entwicklungen hier nicht zu verschlafen. Insbesondere die weltweite Blockchain Insurance Industry Initiative zeigt, dass namhafte Versicherungsunternehmen bereits erheblichen Aufwand betreiben und etwa erforschen, wie mittels der Blockchain-Technologie der Datenaustausch bei Rückversicherungsvorgängen effizienter gestaltet werden kann. Erste Ergebnisse sind bereits in naher Zukunft zu erwarten.<sup>45</sup> Daneben können Smart Contracts aufgrund automatisierter Leistungsausführung Versicherungsprozesse beschleunigen und neue Geschäftsfelder eröffnen.

Die vorhandenen Technologien im Bereich der Blockchain und von Smart Contracts sind sicherlich noch nicht vollkommen ausgereift. Mit großen Schritten dürften jedoch technische Lösungen erarbeitet werden. Auch rechtlich bestehen Unklarheiten und kontroverse Fragen, welche es für eine sichere Anwendung zu lösen gilt. Gerade auch die Entwicklung der regulatorischen Rahmenbedingungen bleibt dabei mit Spannung zu verfolgen.

Wie genau Blockchain und Smart Contracts den Versicherungssektor beeinflussen werden, hängt zwar noch von verschiedenen Variablen ab. Mit ersten bedeutsamen Anwendungen ist aber in jedem Fall innerhalb der nächsten fünf Jahre zu rechnen.

## Literatur

1. Blocher, W.: The next big thing: Blockchain – Bitcoin – Smart Contracts. AnwBl. 66(8), 612–618 (2016)
2. Böhme, R., Pesch, P.: Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. DuD 41(8), 473–481 (2017)
3. Djazayeri, A.: Rechtliche Herausforderungen durch Smart Contracts. jurisPR-BKR (12/2016)
4. Guggenberger, N.: Datenschutz durch Blockchain – eine große Chance. ZD 49–50 (2017)
5. Jacobs, C., Lange-Hausstein, C.: Blockchain und Smart Contracts: zivil- und aufsichtsrechtliche Bedingungen. ITRB 10–15 (2017)
6. Kaulartz, M., Heckmann, J.: Smart Contracts – Anwendungen der Blockchain-Technologie. CR 618–624 (2016)
7. Kaulartz, M.: Die Blockchain-Technologie. CR 474–480 (2016)
8. Kaulartz, M.: Herausforderungen bei der Gestaltung von Smart Contracts. InTeR 201–206 (2016)
9. Kaulartz, M.: Smart Dispute Resolution – Automatisierte Konfliktlösung, Tagungsband DSRI-Herbstakademie (2017), im Erscheinen
10. McLean, S., Deane-Johns, S.: Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero? CRI 97–102 (2016)

<sup>45</sup> „Im Juni will die Blockchain-Initiative B3i erste Ergebnisse veröffentlichen.“, vgl. <http://www.munichre.com/de/media-relations/publications/company-news/2017/2017-02-06-company-news/index.html> (zuletzt abgerufen am 26.7.2017).

11. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Abrufbar unter: <https://bitcoin.org/bitcoin.pdf>
12. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton (2016)
13. Pesch, P., Böhme, R.: Datenschutz trotz öffentlicher Blockchain? DuD **41**(2), 93–98 (2017)
14. Schrey, J., Thalhofer, T.: Rechtliche Aspekte der Blockchain. NJW 1431–1436 (2017)
15. Sorge, C., Krohn-Grimberghe, A.: Bitcoin: Eine erste Einordnung. DuD **36**(7), 479–484 (2012)
16. Stiemerling, O.: Qualifizierte Elektronische Signatur mit dem neuen Personalausweis – Oder: QES mit nPA. ein Selbstversuch (26.8.2014). Abrufbar unter: <http://www.cr-online.de/blog/2014/08/26/qualifizierte-elektronische-signatur-mit-dem-neuen-personalausweis-oder-qes-mit-npa-ein-selbstversuch/>