BaFin Perspektiven

Ausgabe 1 | 2018

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Digitalisierung

Folgen für Finanzmarkt, Aufsicht und Regulierung – Teil I

Inhaltsverzeichnis

Vorwort

Vor fast genau zehn Jahren erreichte die globale Finanzkrise in der öffentlichen Wahrnehmung ihren Höhepunkt. Unter dem Druck der Ereignisse wurden die Weichen von Finanzmarktregulierung und -aufsicht neu gestellt. Neue, europäische Strukturen wurden geschaffen, zugleich einigten sich Gesetzgeber und Regulierer auf stringentere Vorgaben.

Inzwischen sind die großen Regelwerke der Nach-Krisen-Zeit abgeschlossen. Der Wandel in der Finanzbranche ist es nicht. Im Zeitalter von Globalisierung und Digitalisierung wird er sogar Fahrt aufnehmen. Was Aufseher und Regulierer vor immer vielschichtigere Fragen stellt und sie – jenseits der angestammten Gefilde von Recht und Ökonomie – in neue Sphären führt, etwa in die der Informationstechnologie.

In einem derart vernetzten und komplexen Umfeld müssen wir uns noch intensiver als bisher mit Vertretern der Finanzwirtschaft und ihrer Verbände, aber auch mit Verbraucherschützern, Wissenschaftlern, Journalisten und selbstverständlich auch der Politik über grundlegende aufsichtliche und regulatorische Themen austauschen. Dafür wichtige Impulse zu setzen, ist die Absicht unserer neuen Schriftenreihe BaFinPerspektiven, die künftig zweimal im Jahr erscheinen soll. Strategische Fragen und Regulierungsvorhaben sollen, abseits der tagesaktuellen Berichterstattung, beleuchtet und aus verschiedenen Blickwinkeln bewertet werden. Die Schriftenreihe wird in deutscher und in englischer Sprache auf www.bafin.de veröffentlicht.

Schwerpunkt der ersten Ausgabe ist die Digitalisierung. Im Fokus steht unter anderem: der aufsichtliche und regulatorische Umgang mit *Big Data* (BD) und künstlicher Intelligenz (*Artificial Intelligence* – AI). Professor Philipp Sandner, Frankfurt School Blockchain Center, beleuchtet Fragen zur Sicherheit der *Blockchain*. Der Frage, wie die *Blockchain* reguliert werden könnte, gehen zwei Autoren der BaFin in einem Beitrag nach. Zu den strategischen Perspektiven der Banken im digitalen Zeitalter äußert sich Professor Stephan Paul von der Ruhr-Universität Bochum in einem Interview.

Ich würde mich freuen, wenn wir mit unserer Schriftenreihe und den Themen dieser Premierenausgabe auf Ihr Interesse stoßen, und bin gespannt auf Ihre Reaktionen und Meinungen.

Ich wünsche Ihnen viel Freude bei der Lektüre.

Felix Hufeld
Präsident der BaFin

I

Big Data und Künstliche Intelligenz (*Artificial Intelligence*) verändern die Finanzmärkte und werfen aufsichtliche und regulatorische Fragen auf, die es zu beantworten gilt.

Aufsicht und Regulierung in Zeiten von Big Data und künstlicher Intelligenz

Autor

Felix Hufeld,
Präsident, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

1 Einleitung

Begriffe wie *Big Data* (BD) und *Artificial Intelligence* (AI) sind derzeit Gegenstand vielfältiger wissenschaftlicher und gesellschaftlicher Diskussionen. *Big Data* – also die großvolumige Entstehung und schnelle Erfassung einer Vielzahl von Daten aus unterschiedlichen Quellen – ist ein Schlüsselelement für die Anwendungen von Analyseverfahren der künstlichen Intelligenz. Neue technologische Entwicklungen ermöglichen weitreichende Fortschritte etwa bei der Erkennung und Verarbeitung von Sprache und Gesichtern, Texten und Bildern, aber auch bei Prozessautomatisierungen (*Robotic Process Automation*). Das Gleiche gilt für die Erzeugung von Sprache (*Natural Language Generation*). Die Produktivität künstlicher Intelligenz hängt stark von Umfang und Qualität verfügbarer Daten ab, mit denen Algorithmen trainiert und getestet werden. Aus diesem Grund ist es sinnvoll, beide Themen nicht getrennt voneinander zu betrachten und sie im Folgenden unter dem Kürzel „BDAI" zusammenzufassen.

Dass BDAI auch im Wirtschaftsalltag immer relevanter wird, beruht auf drei Faktoren: auf dem bereits erwähnten technologischen Fortschritt, dem Wettbewerb auf den Märkten und dem sich ändernden Verbraucherverhalten. Der technologische Fortschritt setzt den Rahmen dafür, dass BDAI immer kostengünstiger wird und sich einfacher in der Praxis anwenden lässt. So hat die Rechenleistung der Computer exponentiell zugenommen, es steht immer mehr kostengünstiger Speicherplatz zur Verfügung, und die Hardwareleistungen steigen. Insgesamt senken diese Entwicklungen die Technologiekosten und somit auch die Barrieren für die Nutzung von BDAI.

Mit Blick auf die Wettbewerbssituation ist zu beobachten, dass viele Unternehmen vermehrt auf die Auswertung und Nutzung von Daten setzen, um ihre Geschäftsmodelle und -prozesse zu optimieren. Aus dieser Marktsituation heraus sind inzwischen zahlreiche datengetriebene Geschäftsmodelle[1] entstanden. Zudem haben die bequeme Nutzung und die Schnelligkeit der neuen technologischen Möglichkeiten dafür gesorgt, dass

1 Datengetriebene Geschäftsmodelle, die BDAI zur Wertschöpfung nutzen, haben einige Technologieunternehmen zu den am höchsten bewerteten Unternehmen der Welt aufsteigen lassen.

sich viele Verbraucher digitalen Anwendungen zuwenden, und es ist davon auszugehen, dass sich diese Entwicklung fortsetzen wird. So entsteht ein sich selbstverstärkender Kreislauf aus Daten und Anwendungen: Die Möglichkeiten der Vernetzung von Menschen, Maschinen und Prozessen nehmen immer stärker zu.

BDAI-Technologien haben das Potenzial, auch die Finanzbranche tiefgreifend zu verändern. Die Möglichkeiten und Chancen sind enorm. In ihrem Bericht „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“[2] hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) analysiert, welche Veränderungen die verstärkte Anwendung von BDAI für den Finanzmarkt insgesamt, die Unternehmen, die Verbraucher, aber auch für die Aufsicht mit sich bringen könnte. Aufsicht und Regulierung müssen sich frühzeitig mit diesen Veränderungen beschäftigen – auch mit den Risiken, die BDAI-Anwendungen möglicherweise mit sich bringen. Im Folgenden werden die zentralen Herausforderungen von BDAI für die prudenzielle Regulierung und den Verbraucherschutz skizziert.

2 BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, www.bafin.de/dok/10985478, abgerufen am 10.07.2018. Die Studie wurde unter Mitwirkung von PD – Berater der öffentlichen Hand GmbH, der Boston Consulting Group GmbH und Fraunhofer – Institut für Intelligente Analyse- und Informationssysteme erstellt. Der Artikel „Aufsicht und Regulierung in Zeiten von Big Data und künstlicher Intelligenz“ basiert in Teilen auf diesem Bericht.

2 Prudenzielle Regulierung

Betrachtet man aus der Vogelperspektive, wie BDAI funktioniert und wirkt, wird schnell klar, warum BDAI-Anwendungen das Zeug haben, den Finanzmarkt grundlegend zu verändern. Finanzdienstleistungen hängen sehr stark von Informationen und deren Bewertungen ab. BDAI liefert die Möglichkeit, immer mehr und immer präzisere Informationen zu gewinnen. Aus diesen Informationen lassen sich dank BDAI neue Bewertungen erzeugen – etwa zu Asset-Preisen, zur Kreditwürdigkeit und zu einem Risikoprofil für die Krankenversicherung.[3] Sind diese Bewertungen den klassischen Verfahren überlegen, haben Anbieter, die sie nutzen, einen Wettbewerbsvorteil: Wer zum Beispiel die Kreditwürdigkeit einer Person besser einschätzt als sein Konkurrent, kann einen risikoadäquateren Preis verlangen und sich langfristig gegen diesen Konkurrenten durchsetzen. Das Phänomen BDAI wird also einen gewissen Wettbewerbsdruck auslösen, und Unternehmen, die am Markt bleiben wollen, werden nicht umhinkönnen, das eigene Unternehmen für die Nutzung der neuen BDAI-Verfahren fit zu machen.[4]

Der Umstand, dass sich dank BDAI zum einen bislang nicht verfügbare Informationen gewinnen und zum anderen genauere Bewertungen vornehmen lassen, ermöglicht Anbietern, neue Produkte und Dienstleistungen anzubieten – und dies mit potenziell unlimitierter Reichweite. Zum Beispiel lassen sich Ereignisse, deren Eintrittswahrscheinlichkeit vorher nicht oder nur schwer vorhersagbar war, nun durch *Predictive Analytics* vorhersagen. Versicherer können daher – bei entsprechender Nachfrage – ein Produkt zu diesem Ereignis anbieten. Darüber hinaus sind es vor allem die durch BDAI gewinnbaren Informationen über die Kundschaft, die nun eine persönliche Ansprache und personalisierte Produkte ermöglichen. Diese scheinbar persönliche Interaktion via Computer oder Smartphone kennen die Nutzer bereits von vielen Online-Dienstleistern außerhalb der Finanzdienstleistungsbranche, und sie übertragen ihre Erwartungen an diese Dienste auf andere Bereiche, insbesondere auf Finanzdienstleistungen.

Aber auch innerhalb eines Finanzunternehmens gibt es viele Prozesse, in denen Daten entstehen und für Entscheidungen ausgewertet werden müssen. Im Zahlungsverkehr zum Beispiel werden riesige Datenmengen erzeugt und analysiert, um etwa auf Geldwäsche aufmerksam zu werden. Durch den Einsatz von BDAI lassen sich auch bisher unbekannte Muster und Zusammenhänge erkennen – und dies zu deutlich geringeren Kosten. Ein weiteres Beispiel für die Nutzung von BDAI ist die Schadenregulierung bei Versicherern. Immer mehr Entscheidungen lassen sich durch BDAI automatisiert unterstützen und vorbereiten. In der Vergangenheit war es bei der Automatisierung von Prozessen unabdingbar, dass Vorgehensweisen weitgehend vordefiniert waren. Der Algorithmus war nicht anpassungsfähig. Im Rahmen von BDAI werden nun aber vermehrt Algorithmen eingesetzt, die selbstlernend sind. Dies macht es möglich, dass immer komplexere Prozesse (teil)-automatisiert werden. Wettbewerbsdruck – diesmal auf der Kostenseite – könnte ein weiterer Katalysator für die Nutzung von BDAI sein.

Der Einsatz von BDAI kann also auch auf dem Finanzmarkt zu einem entscheidenden Wettbewerbsvorteil werden, und auch die Unternehmen, die unter der Aufsicht der BaFin stehen, werden diesen Vorteil nutzen, um vor allem ihre Effektivität und Effizienz zu steigern. Für die Finanzaufsicht stellt sich daher die Frage, ob und wie die Aufsicht und deren Grundlage, die Regulierung, angepasst werden müssen und an welchen bewährten Prinzipien sie festhalten sollte. Im Folgenden soll auf einige zentrale Aspekte eingegangen werden.

2.1 Wer trägt Verantwortung, der Algorithmus oder der Mensch?

Bei der Aufsicht über ein Unternehmen – zum Beispiel eine Bank – zieht sich ein roter Faden durch die Anforderungen, die die Aufsicht stellt: Alle Entscheidungen, die in der Bank getroffen werden, müssen in eine ordnungsgemäße Geschäftsorganisation eingebettet sein. „Ein Institut muss über eine ordnungsgemäße

3 Vgl. hierzu auch Abschnitt 3.3.

4 Vgl. hierzu aber auch Abschnitt 4.

Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet." So steht es in § 25a Kreditwesengesetz (KWG). Verantwortlich für die ordnungsgemäße Geschäftsorganisation sind nach § 25 a KWG die Geschäftsleiter. Diesen roten Faden, der sich vergleichbar auch durch die Versicherungsaufsicht zieht, wird die Aufsicht auch im Zuge der Ausbreitung von BDAI und der zunehmenden Algorithmisierung nicht durchtrennen: Der Mensch ist und bleibt verantwortlich.

Ist deswegen der Einsatz von Algorithmen verboten? Nein! Jeder einzelne Algorithmus muss aber, genau wie jeder einzelne Mitarbeiter eines Unternehmens, Teil der ordnungsgemäßen Geschäftsorganisation sein. Seine Entscheidungen müssen also innerhalb des Unternehmens und für Dritte nachvollziehbar und damit überprüfbar sein – vor allem dann, wenn sie zentrale und damit risikobehaftete Entscheidungen treffen beziehungsweise diese zumindest vorbereiten. Weder Menschen noch Algorithmen sollten in einem Unternehmen unkontrolliert machen können, was sie wollen.

Entscheidungs- und Bewertungsprozesse können komplexer Natur sein. Sollte BDAI zum Einsatz kommen, kann dies aber nicht bedeuten, dass die Gründe für Entscheidungen im Nachhinein nicht mehr nachvollziehbar sind. Sind neuartige und höchst komplexe Algorithmen am Werk, führen Unternehmen oft sehr schnell das Argument der *Blackbox* an: Der innovative Algorithmus produziere sehr genaue Prognosen, warum und auf welcher Basis er diese tätige, sei aber nicht mehr nachvollziehbar und könne daher leider auch nicht mehr aufsichtlich geprüft werden. Diese Argumentation akzeptiert die Aufsicht nicht, und ein Vorstand wäre gut beraten, sie hausintern ebenfalls nicht zu akzeptieren, da sie auf eine potenziell dysfunktionale Geschäftsorganisation hinweist.

Wie wichtig bei der Nutzung von Algorithmen Erklärbarkeit und Transparenz sind, haben auch Wissenschaft und (angewandte) Forschung bestätigt und dafür Verfahren und Instrumente entwickelt. Auch für komplexe Analyseverfahren gibt es also mittlerweile Möglichkeiten, Erklärbarkeit herzustellen. Man muss also im Finanzsektor nicht auf komplexe Algorithmen und automatisierte Prozesse verzichten, man darf nur nicht vergessen, zugleich auch in deren Transparenz und Erklärbarkeit zu investieren. Als Anreiz sollte den Unternehmen der Umstand dienen, dass nur bei hinreichend transparenten Algorithmen Fehler im Analyseprozess frühzeitig erkannt und behoben werden können, was die Möglichkeiten der Anwendung von BDAI sogar erweitert.

2.2 Aufsichtliche Standards für selbstlernende Systeme

Muss die Aufsicht demnächst aufsichtliche Standards für selbstlernende Systeme definieren? Wird es bald MaAlgo und MaDaten geben – nach dem Vorbild der MaRisk, der Mindestanforderungen an das Risikomanagement der Banken? Eines vorweg: Es geht hier nicht in erster Linie um zusätzliche Regulierung. Nur weil ein Prozessschritt, für dessen Kontrolle die BaFin bisher kein aufsichtsrechtliches Mandat hatte, nun von einem Algorithmus ausgeführt wird und nicht mehr von einem Menschen, heißt das nicht, dass dieser Prozess nun zu regulieren und zu beaufsichtigen ist. Über die Frage, ob und inwieweit die Finanzregulierung zu modifizieren sei, ist an anderer Stelle zu diskutieren. An dieser Stelle geht es um Tatbestände, für deren Überprüfung die BaFin bereits jetzt ein aufsichtsrechtliches Mandat hat. Die entscheidende Frage lautet also: Wie muss sich die Herangehensweise von Aufsicht und Regulierung bei der Überprüfung dieser Tatbestände ändern, wenn hinter ihnen kein Mensch mehr steht, sondern ein Algorithmus?

Im vorangehenden Abschnitt wurde argumentiert, dass Erklärbarkeit und Nachvollziehbarkeit einer algorithmischen Lösung Grundvoraussetzungen für deren Einbettung in eine ordnungsgemäße Geschäftsorganisation seien. Ergebnisse und Prozesse müssen zudem hinreichend dokumentiert werden.

Angenommen, die Grundvoraussetzungen Erklärbarkeit, Transparenz und die Einbettung in eine

ordnungsgemäße Geschäftsorganisation sind für den Einsatz eines Algorithmus gegeben. Welche Standards sollen dann gelten – sei es im Regelbetrieb, sei es in (Re-)Kalibrierungsphasen? Ab wann und wie stark die Aufsicht hier möglicherweise künftig eingreifen muss, sollte natürlich von der Risikorelevanz des jeweiligen Einsatzgebietes abhängen.

An dieser Stelle sollen einige Ideen dazu skizziert werden, wie Unternehmen selbstlernende Algorithmen klug und umsichtig einsetzen könnten: Beispielsweise könnten Unternehmen innovative Ansätze – vor deren Übernahme in den Kundenbetrieb – zunächst in einer geschützten Umgebung kalibrieren, erproben und validieren. In solch einer unternehmensinternen Testumgebung kann das Verhalten eines Algorithmus in verschiedenen Situationen beobachtet und nachvollzogen werden – und dies, ohne dass dadurch ein Schaden entstehen könnte. Bevor BDAI-Lösungen dann tatsächlich zum Einsatz gebracht werden, böte sich an, sie parallel zu bestehenden Systemen laufen zu lassen. Eventuelle Risiken können bei diesem Parallellauf isoliert, quantifiziert und behoben werden. Erst wenn das geschehen ist, sollte die Schleuse zum Live-Einsatz geöffnet werden. Und haben die Algorithmen diese Schleuse erfolgreich passiert, sind weitere Kontrolle und laufende Validierung unabdingbar. Dies insbesondere vor dem Hintergrund, dass selbstlernende Systeme sich stets weiterentwickeln, wenn neue Daten eingespeist werden.

Im Live-Einsatz greifen die Algorithmen häufig auf viele verschiedene Datenströme zu, die unter Umständen auch wieder von Algorithmen erzeugt worden sind. Auf diese Weise kann es zu Entscheidungskaskaden kommen, die sich selbst verstärken. Ein Blick in den Werkzeugkoffer des Kapitalmarkts könnte angesichts dessen nützlich sein: Technische Sicherungsmaßnahmen wie automatische Volatilitätsunterbrechungen sind dort gängige Praxis. Solche automatischen Unterbrecher könnten auch sinnvolle Absicherungsmaßnahmen für algorithmische Entscheidungsprozesse sein – vorausgesetzt, sie selbst sind sinnvoll kalibriert, da andernfalls Fehlentscheidungen und Probleme sogar noch zunehmen könnten.

2.2.1 Konkrete Kalibrierung der Anforderungen

In den vorherigen Absätzen wurde beispielhaft beschrieben, welche allgemeinen Grundvoraussetzungen bei der Nutzung von Algorithmen sinnvoll wären. In bestimmten Situationen könnte es jedoch erforderlich sein, darüber hinaus detailliertere, teils quantitative Anforderungen an die Ergebnisse von BDAI-Anwendungen zu stellen: Wird BDAI zum Beispiel in der Geldwäscheerkennung

eingesetzt, so muss für die Aufsicht überprüfbar sein, ob der Algorithmus hinreichend effektiv ist, also begründete Verdachtsfälle herausfischt, und ob er hinreichend effizient ist, also fehlerarme Verdachtsfälle selektiert. Nur wenn eine Aufsicht auf dieser Grundlage klare Standards definiert hat, welche die Anforderungen an Effizienz und Effektivität beschreiben, kann sie in begründeten Fällen eingreifen und eine Nachjustierung der Modelle verlangen.

2.2.2 Integrität der Daten

So wie die Aufsicht die erwartete Ergebnisqualität klar definieren muss, brauchen Algorithmen ein Feedback zu ihrer Kalibrierung: Der Algorithmus muss wissen, welche Vorhersage richtig war und welche falsch. Hierfür müssen valide beziehungsweise ergebnisrelevante Daten vorliegen. Wer MaAlgo fordert, Mindestanforderungen an Algorithmen, muss also konsequenterweise auch MaDaten fordern (Mindestanforderungen an Daten). Dies ist allerdings mit Blick auf BDAI nicht trivial, zeichnet sich BDAI doch vor allem dadurch aus, dass aus nicht strukturierten Daten wichtige (und richtige) Erkenntnisse erzeugt werden sollen.

Daher muss durch die Unternehmen weiterhin sichergestellt sein, dass für Algorithmen nur valide und ergebnisrelevante Daten verwendet werden. Es wäre ein Mythos zu glauben, dass unternehmerische Entscheidungen nur deshalb objektiv bessere Ergebnisse erzielten, weil sie auf Algorithmen beruhen. Das Gegenteil könnte der Fall sein, denn die Produktion falscher Entscheidungen durch Algorithmen oder unangemessene Inputdaten lassen sich im Zweifel schwerer aufdecken als Fehler in traditionellen Entscheidungsprozessen.

Dieses Problem kann sich dadurch vervielfachen, dass die Reichweite algorithmusbasierter Entscheidungen – also die Zahl der Betroffenen – typischerweise signifikant höher ausfällt als in einer papierbasierten Welt. Fortlaufende Qualitätskontrollen, nicht nur der eingebetteten Algorithmen, sondern auch der verwendeten Daten, werden daher in Zukunft eine deutlich höhere Bedeutung haben als bisher. Aufsicht und Regulierung werden aus diesen Zusammenhängen verlässliche Aufsichtsstandards ableiten müssen.

2.2.3 Beständigkeit genehmigter Anwendungen

BDAI-Modelle zeichnen sich, wie oben beschrieben, unter anderem dadurch aus, dass sie große Datenmengen häufig in Echtzeit zur Vorhersage beziehungsweise Entscheidungsfindung berücksichtigen. Insbesondere über die selbstlernenden Elemente können sich die Modelle beständig weiterentwickeln, indem sie zusätzlichen Dateninput und die darin enthaltenen Erkenntnisse berücksichtigen. Es findet also gewissermaßen fortlaufend eine Anpassung beziehungsweise eine Verbesserung der Modelle und ihrer Kalibrierung statt. Die

Aufsicht muss im Blick haben, dass sich auch Modelle weiterentwickeln können, die sie bereits abgenommen hat. Es stellen sich daher einige grundsätzliche Fragen: beispielsweise die, wie lange eine aufsichtliche Genehmigung Bestand haben kann und wann Modelländerungen im aufsichtlichen Sinne vorliegen. Vor allem aber stellt sich die Frage, wie viel dynamische Anpassung eines Modells gestattet werden kann, damit die Zulassung eines Modells überhaupt möglich ist. Die Aufsicht wird Antworten auf diese Fragen finden müssen – über konkrete Anwendungsfälle und im Dialog mit allen Beteiligten.

2.2.4 BDAI und systemische Risiken: Wen beaufsichtigen wir in Zukunft?

Vielversprechende Verfahren – wie etwa das *Deep Learning* – benötigen riesige Datenmengen („viel hilft viel"), um interessante Ergebnisse zu erzeugen, die wiederum die Grundlage für Produkt- und Prozessinnovationen bilden können. Der Nutzen von BDAI-Verfahren steigt weiter, wenn Unternehmen nicht bloß Informationen über die Präferenzen von Kunden sammeln, sondern auch deren Ausgabeverhalten kennen – zum Beispiel durch den Einblick in Girokonten oder andere Zahlungsverkehrskonten. Dann können ihre BDAI-Algorithmen mit deutlich valideren Daten gefüttert werden. Wer über die Nutzungsrechte an einer Fülle von Daten verfügt, am besten auch von Finanzdaten, hat somit immense Vorteile bei der Entwicklung neuer, vielversprechender BDAI-basierter Produkte und Dienstleistungen – auch und gerade außerhalb des Finanzsektors. Und durch die Nutzung dieser Produkte lassen sich wiederum neue Daten generieren.

Dieser sich selbstverstärkende Kreislauf wird durch das Geschäftsmodell „Bezahlen mit Daten"[5], das einige Bigtechs praktizieren, zusätzlich befeuert. Es könnten sich natürliche Daten- und Auswertungs-Monopole bilden; man spricht in diesem Zusammenhang vom „The-winner-takes-it-all"-Charakter dieser Märkte. Das Bedienen immer neuer Märkte erlaubt es diesen Unternehmen, immer neue Daten aus unterschiedlichen Quellen zu verknüpfen. Durch BDAI-Anwendungen lassen sich somit Portfolio- und Konglomerateffekte[6] erzielen und Verbund- und Skaleneffekte (*economies of scope and scale*) nutzen.

Aufgrund der weiten Verbreitung und der hohen Nutzerzahl könnten dominierende Daten- und Algorithmen-Anbieter, die mit eigenen – möglicherweise quersubventionierten – Finanzdienstleistungen in den Finanzmarkt treten, sehr schnell unmittelbar systemrelevant werden. Solche Anbieter könnten aber auch mittelbar eine relevante Stellung im Finanzsystem erlangen, nämlich dann, wenn sie einer Vielzahl von Finanzmarktakteuren Informationen zum Beispiel für eine genauere Risikokalkulation verkaufen. Vernetzung muss aber nicht zwangsläufig über den Verkauf von Informationen entstehen. Denkbar ist auch, dass Anbieter Finanzmarktakteuren Algorithmen und Infrastruktur(-dienstleistungen) zur Verfügung stellen (siehe auch Szenario „Pooling und Utilities", Seite 16).

Greifen Akteure auf dem Finanzmarkt verstärkt auf Daten oder Algorithmen von nur wenigen großen Anbietern zurück, so kann dies auch makroprudenzielle Folgen haben. Zum einen würde sich eine sehr starke Abhängigkeit von diesen Anbietern ergeben: Was passiert zum Beispiel, wenn die Daten und Modelle fehlerhaft sind oder Infrastrukturen bei diesen Anbietern ausfallen? Zum anderen kann sich auf diese Weise unter Umständen eine prozyklische Wirkung entfalten, wenn eine große Masse an Finanzmarktakteuren aus bestimmten Ereignissen die gleichen Schlüsse und Handlungs- und Handelsstrategien ableitet, weil sie die gleichen Algorithmen verwendet. Eine Analogie zu der Rolle der Rating-Agenturen drängt sich auf.

5 Bei diesem Modell werden Nutzern unter dem Motto „you can not compete with free" vermeintlich kostenlos Dienstleistungen angeboten. Tatsächlich bezahlt der Nutzer die Dienstleistungen, indem er das Nutzungsrecht an seinen Daten vergibt. Problematisch ist dabei vor allem, dass vielen Nutzern der Wert ihrer Daten und somit der Preis, den sie zahlen, nicht hinlänglich bekannt ist.

6 Auszug aus dem Hauptgutachten XX (2012/2013) der Monopolkommission, Kapitel I – Aktuelle Probleme der Wettbewerbspolitik, Seite 63, http://www.monopolkommission.de/images/PDF/HG/HG20/1_Kap_1_A_HG20.pdf, abgerufen am 15.06.2018.

Solche Risiken können durch *Insourcing*, *Outsourcing* oder sonstigen Bezug von BDAI-gestützten Dienstleistungen von Dritten entstehen. Gerade wenn diese Risiken nicht mehr innerhalb der Organisationsstruktur beaufsichtigter Unternehmen liegen, besteht die Gefahr, dass sie nicht mehr vollständig identifiziert und gesteuert werden können. Insgesamt muss man also die Frage stellen, ob die Definition der Systemrelevanz im aufsichtlichen Sinne und damit die Möglichkeit, mitigierende Maßnahmen einzuleiten, an die hier beschriebenen neuen Gegebenheiten angepasst werden muss.

Eng damit verbunden ist die Frage, wer oder was in einer BDAI-Welt welcher Art von (Finanz-)Aufsicht unterliegen muss. Müssen zum Beispiel zukünftig auch solche Anbieter unter Aufsicht gestellt werden, die strukturell Wissen und Informationen in den Finanzmarkt liefern, obwohl sie selbst keine Finanzdienstleistungen erbringen? Hier könnte man einen aus der Marktaufsicht bekannten Gedanken fruchtbar machen und Wohlverhaltenspflichten auch für solche Unternehmen etablieren und beaufsichtigen, die nicht der Institutsaufsicht der BaFin unterliegen.

Szenario

Pooling und Utilities

BDAI kann das *Pooling* von Daten, Technologie und Expertise sowie die Nutzung von *Utilities* fördern, denn der Erfolg von BDAI-Anwendungen steht und fällt mit zwei zentralen Voraussetzungen: Daten und Technologie (und der entsprechenden Auswertungsexpertise). Beide Voraussetzungen sind nicht immer gegeben. Verfügen einzelne Unternehmen beispielsweise nicht über eine ausreichende Datenmenge, um BDAI sinnvoll einsetzen zu können, kann es sich anbieten, dass sie ihre Datenpakete in pseudonymisierter und anonymisierter Form zusammenführen. Denkbar wäre zum Beispiel, dass in einem einzelnen Unternehmen zu wenige Datenpunkte für ein erforderliches Feedback der (selbstlernenden) Algorithmen vorliegen und/oder deren Kalibrierung schwierig ist. Wenn mehrere Unternehmen ihre Daten poolen, steigt die relevante Fallzahl eher auf die erforderliche kritische Masse. Die Daten stehen somit für datengetriebene Innovation in ausreichender Menge zur Verfügung.

Das *Pooling* – sowohl von Daten als auch von Technologie und Fachwissen – ist aber nur möglich, wenn die technischen, organisatorischen und juristischen Voraussetzungen erfüllt sind. Insbesondere beim *Pooling* von Daten ist zudem entscheidend, dass die Datensouveränität der einzelnen Unternehmen garantiert werden kann. Hierzu gibt es zum Beispiel die von Wirtschaft, Politik und Forschung 2014 gemeinschaftlich ins Leben gerufenen Initiative „Industrial Data Space".

BDAI-Anwendungen könnten somit die Bedeutung von *Utilities* steigern, also von Vehikeln, in denen sich mehrere Unternehmen zusammenschließen, um bessere Auswertungen zu ermöglichen, Kostenvorteile zu erzielen und gleichgerichtete Interessen zu verfolgen. Vor allem in der Finanzbranche können zudem durch gemeinsame Nutzung von Expertise und gemeinsam entwickelte Lösungen aufsichtliche und regulatorische Anforderungen zielgerichteter erfüllt werden (zum Beispiel Regtech-Anwendungen, Geldwäscheprävention, Know-your-customer-Prozesse). BDAI kann diese Entwicklung antreiben. Ziel ist es, entscheidende Verbund- und Skaleneffekte zu realisieren.

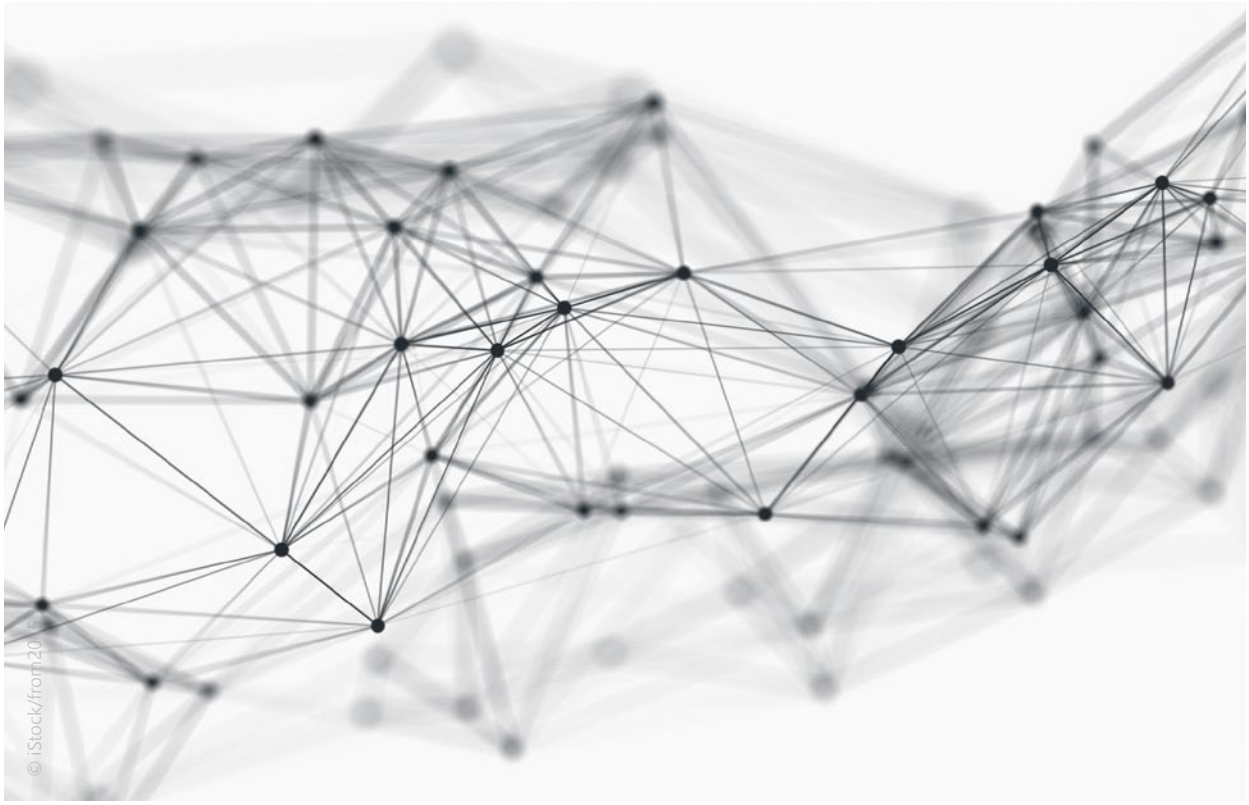
Die Aufsicht muss sich die Frage stellen, wie bei zunehmendem *Pooling* und einer wachsenden Nutzung von *Utilities* neu auftretende Risiken angemessen zu erfassen und zu adressieren sind.

3 Verbraucherschutz

3.1 Das digitale Revival des Tante-Emma-Prinzips

Zunächst ist festzustellen, dass der Einsatz von BDAI durchaus Vorteile für Kunden und Verbraucher haben kann. Ein Blick zurück in die jüngere Vergangenheit zeigt dies: Bis in die 1980er Jahre hinein versorgten vor allem kleine Läden die Bevölkerung lokal mit Lebensmitteln und anderen Produkten des täglichen Bedarfs. Wer einen solchen Tante-Emma-Laden führte, genoss das Vertrauen seiner Kunden und hatte mitunter tiefe Einblicke in deren Privatleben. Kaufleute kannten also die Wünsche und Bedürfnissen ihrer Kunden, konnten ihnen individuelle Angebote unterbreiten und die Geschäfte schnell und unkompliziert abwickeln. Wollte Herr X zum Wochenende immer frischen Lachs kaufen, ein Produkt, das ansonsten aufgrund der geringen Nachfrage nicht im Angebot war, konnte der Kaufmann jeden Freitag eine bestimmte Menge Lachs in seine Produktpalette aufnehmen. Von solchen zugeschnittenen Angeboten profitierten beide Seiten. Die Kundenzufriedenheit war hoch, die Kundenbindung eng. Sie ging sogar so weit, dass der Kunde anschreiben lassen konnte, wenn er kein Geld dabei hatte. Diese Vorteile gingen mit dem Aufkommen der Supermärkte verloren. Der klassische Trade-off zwischen Informationsverbreitung und -tiefe galt. Internet und Digitalisierung erlauben es nun, dieses Paradigma aufzulösen.

Das Tante-Emma-Prinzip lässt sich heute im Grunde auf alle Lebensbereiche übertragen und skalieren. Voraussetzung: ein tiefes Verständnis von den Anforderungen und Bedürfnissen der einzelnen Kunden. BDAI liefert hierfür den Werkzeugkasten, ohne in persönliche Beziehungen zwischen Einzelpersonen eintreten zu müssen, jedoch mit der Möglichkeit, auf sehr persönliche Daten zuzugreifen. BDAI macht also, vereinfacht gesprochen, ein großflächiges Revival des Tante-Emma-Prinzips möglich – und zwar in allen Branchen. Die entscheidende Frage lautet, ob Anbieter und Kunden von diesem Revival gleichermaßen profitieren.



Ein weiterer Blick zurück in die Zeit der Tante-Emma-Läden: Was machte damals die Beziehung zwischen Kunden und Kaufmann aus? Es war stets der Kunde, der entschied, ob und was er dem Kaufmann von sich preisgab. Hinzukam: Die mitunter sehr privaten Informationen standen (im Idealfall) nur dem Kaufmann zur Verfügung, und der Kunde behielt die Kontrolle und den Überblick darüber, was der Kaufmann über ihn wusste. Die vertrauensvolle Beziehung zwischen Kunden und Händlern war mancherorts mit der Beziehung zum Arzt, Seelsorger oder Anwalt vergleichbar. Der Einzelhändler konnte sich auf diese Weise ein umfassendes Bild von der Persönlichkeit seines Kunden, seinen Lebensumständen und seinen Wünschen und Bedürfnissen machen. Verletzte er das Vertrauen seines Kunden, konnte dies für ihn erhebliche geschäftliche und vor allem auch persönliche und gesellschaftliche Konsequenzen haben. Die Machtverhältnisse zwischen Kunden und Kaufmann waren also in der analogen Welt gut austariert, und der Händler konnte sein Wissen fast ausschließlich für seine eigenen geschäftlichen Ziele nutzen. Für Dritte war sein Wissen wertlos, denn er konnte es nicht ohne weiteres verkaufen.

All dies hat sich im Zuge der Digitalisierung und durch das Entstehen neuer Geschäftsmodelle (*eCommerce*, Plattformwirtschaft und virtuelle Netzwerke) grundlegend geändert. Auch ohne aufwändige Face-to-Face-Interaktion lassen sich heute die Bedürfnisse und Wünsche von Kunden tiefgehend automatisiert analysieren. Der Einsatz von BDAI macht persönliche Beziehungen für die Erkenntnisgewinnung überflüssig, nicht aber persönliche Daten. Der Verbraucher hat es nicht mit einem konkreten Gegenüber zu tun, das er kennt, dem er vertraut und das ihn genau analysiert. Auch ist ihm nicht bewusst, wofür seine Daten verwendet werden könnten und welchen Wert sie haben. Hinzukommt, dass er nur sehr schwer ausmachen kann, ob er möglicherweise aufgrund seiner Daten diskriminiert wird.[7]

Statt des persönlichen Kontakts ist es in der BDAI-Welt für die Gewinnung des oben beschriebenen Wissens nun vor allem erfolgsentscheidend, eine kritische Masse an Nutzern zu erreichen und Netzwerk- und Konglomerateffekte zu realisieren. Aus den dadurch massenhaft verfügbaren Nutzerdaten werden die erforderlichen Datenmengen als Input für die neuen Auswertungsmethoden (zum Beispiel *Deep Learning*) generiert. Die Erkenntnisse zu den Präferenzen der Kunden können zunächst die Unternehmen selbst zur zielgenauen Vermarktung von Produkten und zur persönlichen Ansprache einsetzen. Neu ist aber, dass diese Erkenntnisse nun auch für Dritte wertvoll sind, dass die Unternehmen sie also verkaufen können. Sehr persönliche Informationen können – auch Dritten gegenüber – monetarisiert werden. Der Kunde verliert dabei schnell den Überblick darüber, welches Unternehmen was über ihn weiß und wozu letztendlich die Daten genutzt werden, die er ursprünglich freigegeben hat. Vorbei ist also die Zeit der austarierten Machtverhältnisse: BDAI kann signifikante Macht- und Informationsasymmetrien zwischen Kunden und Unternehmen zur Folge haben.

In diesem Zusammenhang sind finanzwirtschaftliche Daten für Unternehmen besonders interessant, da sie den ökonomischen Kern einer Person offenlegen: Einkommen, Vermögen, Zahlungsverkehr/Ausgabeverhalten, Vertragsbeziehungen, Gesundheitsstatus usw. Auch der Besitzer des Tante-Emma-Ladens wäre an diesen detaillierten Informationen interessiert gewesen, konnte er doch nur ungenaue Schlüsse ziehen, etwa aus Kleidung und Beruf seines Kunden. Weil Finanzdaten besonders sensibel sind, gaben und geben Kunden sie aber nur sehr ungern und sparsam preis – und das auch nur ausgewählten Vertrauenspersonen. Zudem hätte der Krämer schwerlich die maximale Zahlungsbereitschaft seiner Kunden ausnutzen können. Er konnte schließlich nicht permanent seine Preisschilder anpassen, etwa wenn der zahlungskräftige und anspruchsvolle Kunde B den Laden betrat, während er den weniger zahlungskräftigen Kunden A noch bediente. Im Internet ist aber genau das schnell getan. Der Rohstoff Finanzdaten kann also für Unternehmen in der heutigen Zeit ein entscheidendes Mittel zur Gewinnmaximierung darstellen – möglicherweise auch zu Lasten des Kunden (siehe Szenario „Maximale Abschöpfung der Zahlungsbereitschaft zur Gewinnmaximierung“, Seite 24).

7 Vgl. hierzu Abschnitt 3.3.

Der Kunde muss aber aus Sicht des Verbraucherschutzes auch heute noch in der Lage sein, selbst darüber zu entscheiden, wem er seine Daten für welche Zwecke weitergibt. Gerade wenn es um Finanzdaten geht, ist Datensouveränität wichtig. Zudem gilt es darauf zu achten, dass die neuen Möglichkeiten der Erkenntnisgewinnung nicht gegen die Verbraucher eingesetzt werden. Zwischen erlaubter und legitimer Differenzierung und unerlaubter Diskriminierung verläuft ein schmaler Grat.[8] Die gängigen Sammel- und Auswertungsaktivitäten, wie sie bei manchen Online-Diensten und anderen datengetrieben Geschäftsmodellen üblich sind, lassen sich sicherlich nicht 1:1 auf Finanzdaten übertragen.

Im Folgenden soll daher auf zwei zentrale Fragen in diesem Zusammenhang eingegangen werden:

- Wie kann ein Kunde auch in der neuen BDAI-Welt die Kontrolle über seine Daten behalten? Mit anderen Worten: Wie lässt sich Datensouveränität unter den Bedingungen massenhafter und selbstlernender Datenauswertung gewährleisten?
- Und wie kann auch unter BDAI-Bedingungen ein diskriminierungsfreier Zugang zu Finanzprodukten gewährleistet werden?

8 Vgl. hierzu Abschnitt 3.3.

3.2 Datensouveränität unter den Bedingungen massenhafter und selbstlernender Datenauswertung

Wie also lässt sich Datensouveränität unter den Bedingungen massenhafter und selbstlernender Datenauswertung gewährleisten? Die wesentlichen Voraussetzungen für Datensouveränität sind eine angemessene und transparente Aufklärung über die Datennutzung und die potenziellen Konsequenzen, verlässliche Kontrollmöglichkeiten (auch im Nachhinein) und tatsächliche Wahlfreiheit.

3.2.1 Angemessene und transparente Aufklärung

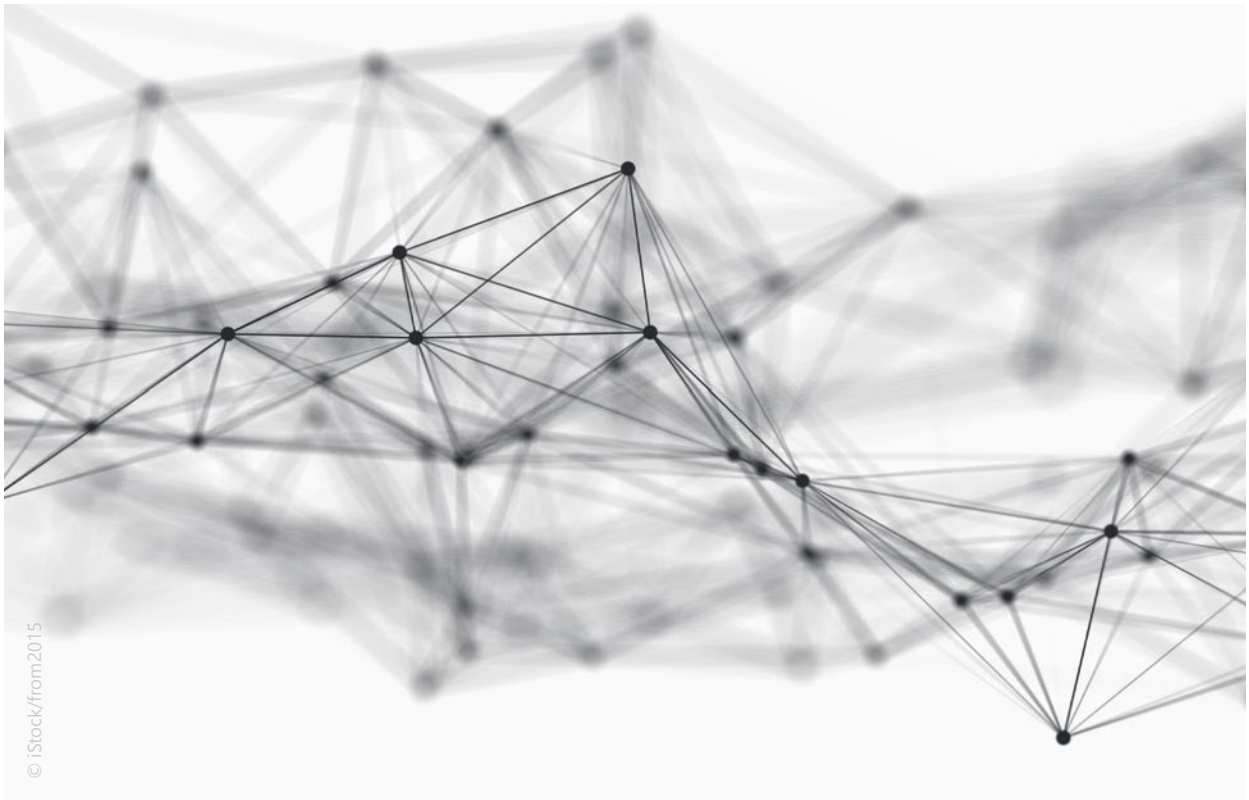
Um souverän entscheiden zu können, muss ein Kunde zunächst verstehen, wofür er seine Daten freigeben soll und welche Nutzungsmöglichkeiten sich hieraus für das Unternehmen ergeben. Er muss also die möglichen Konsequenzen einer Datenfreigabe einschätzen können. Hierüber muss der Kunde angemessen und transparent aufgeklärt werden. Zu beachten ist hierbei, dass Kunden Datenschutzbestimmungen meist nicht lesen, wenn sie diese als unklar und schwer verständlich empfinden. Datenschutzbestimmungen müssen daher verständlich formuliert und der spezifischen

Entscheidungssituation angepasst werden. Das Forschungszentrum Informatik (FZI) schlägt in seinem Bericht „Smart Data – Smart Privacy?“ beispielsweise vor, dem Verbraucher die Ergebnisse der Datenschutzfolgenabschätzung (gemäß. Art. 35 der europäischen Datenschutz-Grundverordnung – DSGVO) in vereinfachter Form als Entscheidungsgrundlage für eine Datenpreisgabe zur Verfügung zu stellen.[9] Das FZI vertritt zudem die Meinung, ein einheitliches, einfach verständliches Skalensystem oder ein intuitives Ampelsystem, aus dem hervorgehe, mit welchen Risiken die Datennutzung verbunden ist, sei eine gute Möglichkeit, den Kunden aufzuklären.

Der deutsche Sachverständigenrat für Verbraucherfragen schlägt eine Datenschutzerklärung als One-Pager vor, um den Kunden schnell und einfach zu informieren.[10] Solche vereinfachten Darstellungen scheinen auch aus Sicht eines Finanzaufsehers – zumindest als Ergänzung zu den bisherigen Datenschutzerklärungen – ein vielversprechender Weg zu sein, über den man intensiver nachdenken sollte (siehe auch Exkurs „Potenzielle Berührungspunkte der Finanzaufsicht mit Datenschutzfragen“, Seite 21).

9 FZI Forschungszentrum Informatik, Smart Data – Smart Privacy? Impulse für eine interdisziplinär rechtlich-technische Evaluation, Seite 13 f., https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.pdf?__blob=publicationFile&v=7, abgerufen am 11.06.2018. Die Erstellung des Thesenpapiers wurde vom Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des deutschen Bundestages gefördert.

10 Sachverständigenrat für Verbraucherfragen, Digitale Souveränität – Gutachten des Sachverständigenrats für Verbraucherfragen, http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf, abgerufen am 11.06.2018.



Exkurs

Potenzielle Berührungspunkte der Finanzaufsicht mit Datenschutzfragen

Eine der Aufgaben der BaFin besteht darin, im Rahmen der ihr gesetzlich zugewiesenen Kompetenzen dafür zu sorgen, dass Marktteilnehmer und Verbraucher in die Funktionsfähigkeit, Stabilität und Integrität des Finanzmarktes vertrauen können.

Geht es um Kundendaten, die mehr und mehr zum Wirtschaftsgut werden, wird der Kunde zugleich zum Datenlieferanten, und es muss dafür gesorgt werden, dass die Interessen aller Marktteilnehmer (auch der Verbraucher) gleichermaßen berücksichtigt werden.

Dies zu überwachen, ist primär Aufgabe der Datenschutzbehörden. Es können sich allerdings Fallgestaltungen ergeben, in denen auch die Finanzaufsicht unmittelbar zum Handeln aufgefordert sein könnte:

- Nach der Ende Mai 2018 in Kraft getretenen europäischen Datenschutz-Grundverordnung (DSGVO) können die von der BaFin beaufsichtigten Unternehmen bei Datenschutzverstößen mit hohen Geldstrafen belegt werden. Da diese Geldbußen im Extremfall auch die Solvenz eines Unternehmens beeinträchtigen können, sind Datenschutzverstöße insoweit auch für die Finanzaufsicht ein Thema.
- Häufen sich Datenschutzverstöße in systematischer Form, könnte dies Zweifel an der Ordnungsgemäßheit des Geschäftsbetriebs wecken und einen Missstand darstellen, den die Finanzaufsicht gegebenenfalls beheben muss.
- Sollte ein Unternehmen, das von der BaFin beaufsichtigt wird, im Umgang mit Kundendaten einschlägige Regularien systematisch und absichtsvoll missachten, könnte dies in bestimmten Fällen auch die Eignung der Geschäftsleitung in Frage stellen.

3.2.2 Verlässliche Kontrollmöglichkeiten

Auch nachdem ein Nutzer seine Daten freigegeben hat, muss er die Kontrolle über seine Daten behalten können. Er muss also überblicken können, wem er welche Daten freigegeben hat, er muss sich über die Verwendung seiner Daten informieren können, und es muss möglich sein, dass er eine Datenfreigabe unkompliziert wieder zurückzunehmen kann. Das Recht auf Löschung der Daten, auf deren Vergessen, muss gewährleistet sein.

Eine Idee, wie sich der Kunde einen Überblick über die Verwendung seiner Daten verschaffen kann beziehungsweise wie Unternehmen dies ermöglichen können, besteht darin, bei der Gestaltung von Datenbanken und Datenmanagementsystemen eine automatisierte Protokollierung zu implementieren. So könnte man beispielsweise jedem Datum eine Notiz anhängen. Diese Notiz gäbe an, für welche Auswertungen dieses Datum von wem benutzt werden darf. Möchte ein Algorithmus nun auf das Datum zugreifen, so geht dies nur, wenn die Notiz ihm einen Zugriff erlaubt. Darüber hinaus kann für jedes Datum mit einem entsprechenden Logfile automatisch darüber buchgeführt werden, wer (zum Beispiel welcher Algorithmus) wann und wozu auf das jeweilige Einzeldatum zugegriffen hat.

Dank solcher Lösungen, die im klassischen Datenmanagement in anderen Zusammenhängen üblich und erprobt sind, behält ein Unternehmen den Überblick über die Nutzung der Kundendaten und kann sowohl die Daten- als auch Nutzungsprofile verwalten. Somit kann ein Unternehmen, das über ein derartiges Datenmanagementsystem verfügt, sehr schnell Auskunft darüber geben, wie, wann, für welchen Zweck und von wem Kundendaten verwendet wurden. Widerruft der Kunde seine Einwilligung in die Datennutzung, ist auch

dies relativ schnell umsetzbar. Der deutsche Sachverständigenrat für Verbraucherfragen empfiehlt darüber hinaus, ein verbraucherzentriertes Datenportal einzurichten.[11] Ein solches Portal könnte Verbrauchern mehr Kontrolle über die Nutzung ihrer individuellen Daten durch verschiedene Anbieter geben. Ziel ist es, dass der Verbraucher seine Daten zentral löschen und ändern und – darüber hinaus – seine Zugriffsrechte zentral verwalten kann.

3.2.3 Tatsächliche Wahlfreiheit

Über Aufklärung und Kontrolle hinaus ist für Datensouveränität entscheidend, dass man dem Kunden tatsächlich Wahlfreiheit gewährt, was die Nutzung seiner Daten angeht. Das Grundprinzip einer jeden souveränen Entscheidung ist eine gangbare Alternative: Wer keine echte Wahl hat, trifft keine Entscheidung und erst recht keine souveräne. Der Kunde darf also nicht de facto gezwungen werden, einer weitreichenden Nutzung seiner Daten zuzustimmen, er muss (mindestens) eine Alternative haben. Eine spannende Frage hierzu lautet, wie diese Alternativen konkret aussehen müssen, damit von einer souveränen Entscheidung gesprochen werden kann. Reicht es aus, wenn grundsätzlich am Markt auch Produkte verfügbar sind, für die der Kunde eine weniger weitreichende Freigabe seiner Daten erteilen muss? Oder muss jedes einzelne Unternehmen auch alternative Produkte anbieten? Wie müssten diese alternativen Produkte beschaffen sein? Sie hätten wahrscheinlich nicht dieselben Features wie die Produkte, für die der Kunde eine weiterreichende Freigabe erteilen muss. Dennoch sollten sie für den Kunden nicht gänzlich unattraktiv sein, denn dann bestünde keine echte Wahlfreiheit.

Es wäre darüber hinaus auch denkbar, dass Unternehmen Kunden die Möglichkeit geben, die Nutzung ausgewählter Daten für einen klar definierten Zweck und innerhalb eines begrenzten Zeitraums freizugeben. Viele BDAI-Anwendungen könnten zudem über ein Privacy-preserving *Data Mining* erfolgen, also auf der Grundlagen anonymisierter Daten.

Friss-oder-stirb-Situationen, in denen der Kunde nur die Wahl hat zwischen einer sehr weitreichenden Datenfreigabe und dem Verzicht auf ein Produkt oder eine Dienstleistung, haben jedenfalls mit Wahlfreiheit nichts zu tun. Essenziell ist, dass sich der Kunde generell gegen eine Datennutzung entscheiden kann, wenn sie über das Maß hinausgeht, das für die Vertragserfüllung erforderlich ist.

Auch wenn Menschen zusätzlich Daten aus sozialen Medien, Apps und Portalen freigeben müssen, um noch zu vertretbaren Konditionen Zugang zu Finanzprodukten zu erhalten, kann von souveränen Entscheidungen nicht mehr die Rede sein. Denn Kunden, die dies nicht wünschen oder über diese Daten nicht verfügen (wie wenig digitalisierungsaffine Kunden), wären stark benachteiligt.

3.3 Diskriminierungsfreier Zugang zu Finanzprodukten unter BDAI-Bedingungen

Differenzierung anhand persönlicher Daten ist üblich und grundsätzlich sinnvoll. Will ein Kunde zum Beispiel eine Autoversicherung abschließen, ist der Versicherer nach geltendem Aufsichtsrecht ausdrücklich aufgefordert, dafür einen risikoadäquaten Preis zu verlangen. Die schwierige Frage lautet: Ab wann hören sinnvolle und gewünschte Risikoadäquanz und Differenzierung auf und ab wann beginnt Diskriminierung, die lediglich der Gewinnmaximierung dient (siehe auch Szenario „Wohin kann Differenzierung führen?“, Seite 23)?

11 Sachverständigenrat für Verbraucherfragen, a.a.O. (Fn. 10).

Szenario

Wohin kann Differenzierung führen?

Die neuen Prognosemöglichkeiten, die BDAI bietet, können mit der Zoom-in-Funktion hochauflösender Bildschirme verglichen werden: Wo früher nur ein grobes Bild zu sehen war, entstehen nun im Detail sehr scharfe Bilder, die fast beliebig vergrößert und analysiert werden können. Die mit BDAI einhergehenden Möglichkeiten der Differenzierung sind also nicht gänzlich neu, sie sind aber wesentlich besser und genauer als ältere Verfahren.

Ein Beispiel ist die Risikoprüfung bei der Krankenversicherung: BDAI könnte eine noch signifikant genauere Prognose der Gesundheitsrisiken eines Menschen erlauben. Allein die klassischen Informationskanäle wie etwa Arztberichte könnten durch BDAI besser ausgewertet werden. BDAI macht es aber auch möglich, die Erkenntnisse aus den Arztberichten mit Informationen aus den sozialen Medien zu kombinieren. Durch diese zusätzlichen Daten, die in vielen Fällen von den Kunden selbst bereitgestellt werden, wird eine immer präzisere Risikodifferenzierung möglich. Unabhängig davon besteht die Chance, dass BDAI die medizinischen Diagnose- und Prognosemöglichkeiten weiter verbessert – Stichwort *„Predictive Analytics"*. Wohin werden diese Entwicklungen führen?

Wird künftig eine dermaßen präzise Risikoprognose und -differenzierung möglich sein, dass wesentliche Kundengruppen aus den – korrekt bepreisten – Kollektiven faktisch ausgeschlossen werden, weil sie sich eine Versicherung ihrer (nun besser einschätzbaren) Risiken nicht mehr leisten können? Werden sich künftig nur noch Menschen mit „guten" Risiken versichern können? Wer wird dann die Risiken der anderen tragen, die bislang Teil eines versicherungstechnischen Kollektivs sind? Die Gesellschaft, sprich: der Steuerzahler?

Es ist davon auszugehen, dass eine weitreichende BDAI-gestützte Risikoselektion zu gesellschaftlichen Debatten führen wird, die zwar nicht grundsätzlich neu sind – Stichwort „Versicherbarkeit von Terrorgefahren", in der sich abzeichnenden Dimension aber eine andere Qualität erreichen werden. Möglicherweise wird auch in der Finanzwirtschaft künftig nicht alles sinnvoll oder akzeptabel sein, was technisch möglich ist.

Auch unter BDAI-Bedingungen muss es gelingen, eine angemessene Balance zwischen notwendiger Differenzierung und nicht gewünschter Diskriminierung zu finden und einen diskriminierungsfreien Zugang zu Finanzprodukten zu gewährleisten. BDAI ermöglicht, wie oben erwähnt, einen sehr tiefen Einblick in die Privatsphäre von Kunden, also etwa in ihre Präferenzen, ihre Wünsche und ihre Zahlungsfähigkeit und -bereitschaft. Diese Informationen können im Sinne des Kunden dazu genutzt werden, ihm Produkte und Dienstleistungen auf den Leib zu schneidern. Sie können aber auch bewusst gegen den Verbraucher verwendet werden oder ihm zumindest zum Nachteil geraten. Ein Anbieter, der sehr viel über eine Person weiß, kann diese Informationen ausnutzen, um beispielsweise deren Zahlungsbereitschaft auch in Abhängigkeit von spezifischen Lebenssituationen maximal abzuschöpfen (siehe auch Szenario „Maximale Abschöpfung der Zahlungsbereitschaft zur Gewinnmaximierung", Seite 24). Er kann auch bewusst Kunden(-gruppen) ausschließen, indem er Preise festsetzt, die über deren Zahlungsfähigkeit und -bereitschaft hinausgehen. Neben dieser bewussten Diskriminierung einzelner Verbraucher(-gruppen) kann es aber auch zu einer unbewussten Diskriminierung kommen, weil der Algorithmus diskriminierende Entscheidungen trifft, ohne dass der Anwender ihn explizit entsprechend programmiert hätte.
Auf beide Arten der Diskriminierung und die Frage, wie sie sich vermeiden lassen, soll im Folgenden eingegangen werden.

Szenario

Maximale Abschöpfung der Zahlungsbereitschaft zur Gewinnmaximierung

Man stelle sich ein Online-Einkaufszentrum der Zukunft vor. In dem Moment, in dem der Kunde es betritt, wird ihm eine Fülle von Produkten und Dienstleistungen angeboten, die fast ausnahmslos zu seinem Geschmack, seiner Lebenssituation und seinen momentanen Bedürfnissen passen. Der Kunde ist begeistert. Er braucht nur noch auf „kaufen" zu klicken. Der Preis passt, wenn er auch nahe an dem Preis liegt, den er gerade noch zu zahlen bereit ist. Da das Produkt oder die Dienstleistung speziell auf ihn zugeschnitten ist, sind direkte Preisvergleiche erschwert.

An diesem hypothetischen Szenario lässt sich verdeutlichen, worin für Unternehmen – neben der Ausweitung von Produktangeboten und Marktanteilen – ein weiterer Vorteil von BDAI-Anwendungen liegen kann: BDAI bietet bisher nicht dagewesene Möglichkeiten, die Konsumentenrente[12] abzuschöpfen. Was für die Unternehmen ein Segen wäre, kann allerdings zum Fluch für die Nutzer und Verbraucher werden.

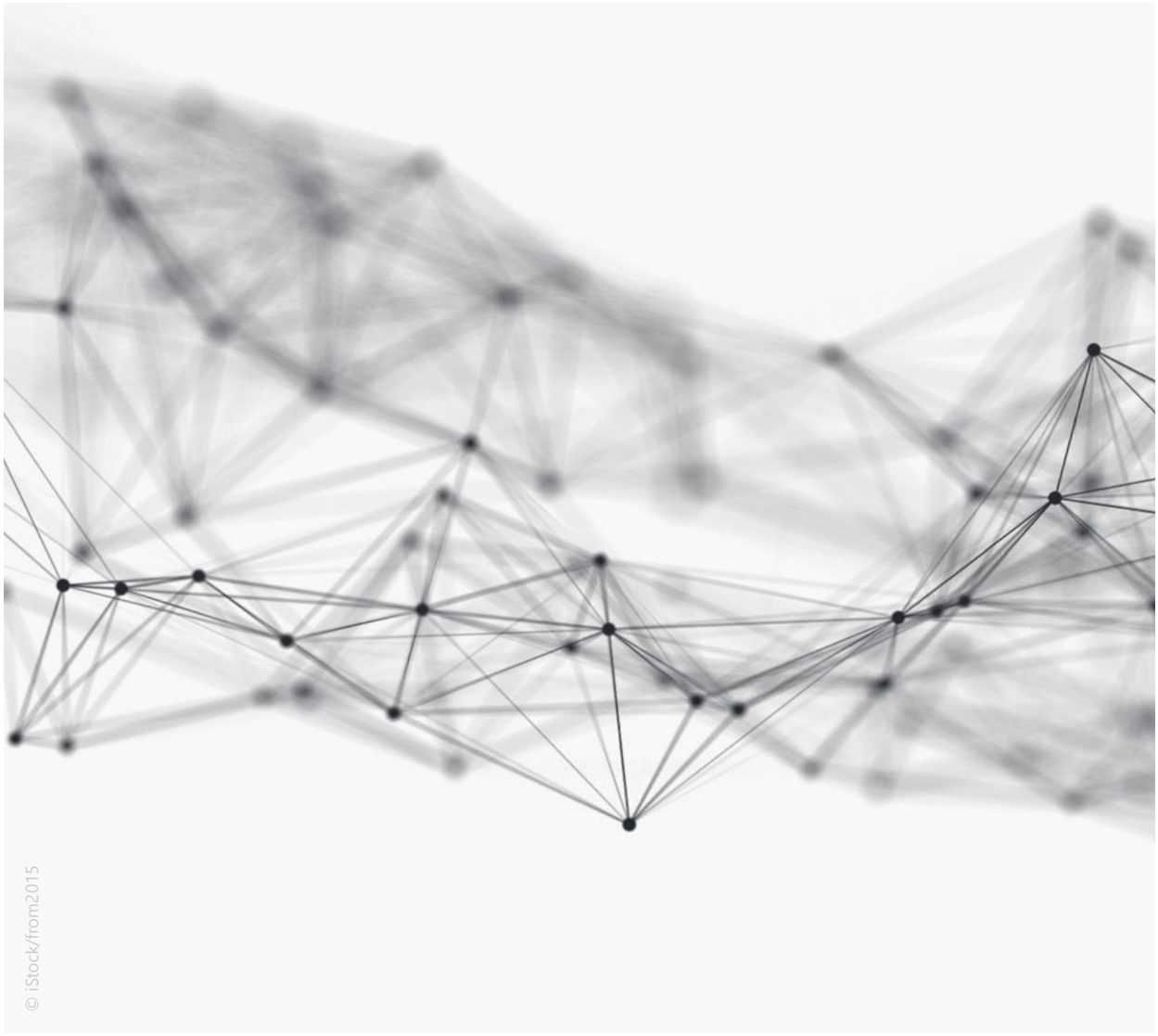
Vor allem die BDAI-gestützte Verknüpfung von Daten zu Bedürfnissen und Präferenzen mit finanzwirtschaftlichen Transaktions- und Verhaltensdaten kann sehr tiefe Einblicke in bislang verborgene Verbrauchercharakteristika ermöglichen – etwa in die (situative) Zahlungsbereitschaft und -fähigkeit. Dieses intime Wissen kann auch gegen Verbraucherinteressen eingesetzt werden. Es liegt im ökonomischen Interesse des Verbrauchers, dass Anbietern zumindest seine Zahlungsbereitschaft und, in Grenzen, seine Zahlungsfähigkeit verborgen bleiben.

Ansonsten besteht die Gefahr, dass Verbraucher, beziehungsweise das Verbraucherkollektiv, beim Einsatz von BDAI strukturell überteuerte Produkte kaufen. Unternehmen können mit Hilfe von BDAI tiefe Kenntnisse über die preislichen Schmerzgrenzen breiter Verbrauchergruppen gewinnen – entweder weil sie selber über diese Daten verfügen oder indem sie sie zukaufen. Es besteht die Gefahr, dass Unternehmen dieses Wissen zur Ertragssteigerung gezielt ausnutzen. Denn über diese extreme Preisdifferenzierung (*Segment of One*) können sie über höhere Preise deutlich höhere Gewinne realisieren, ohne Einbußen bei der abgesetzten Menge befürchten zu müssen.

Dabei geht es nicht um das Zahlen höherer Preise für bessere oder passendere Leistungen, also etwa um höhere Versicherungsprämien für die Absicherung höherer Risiken. Dies wäre eine auch aufsichtlich gewollte Differenzierung. Es geht um individuelle und situative Bepreisung (annähernd) gleicher Produkte. BDAI-Anwendungen können die kostengünstige Entwicklung (massen-)individueller Produkte und Dienstleistungen erleichtern: Anbieter können Standardprodukte – ohne tatsächliche Mehrleistung – mit individualisierten Bestandteilen versehen, womit sie es Verbrauchern schwerer machen, zu vergleichen oder auf andere Angebote beziehungsweise Anbieter auszuweichen.

Klar ist: Preisdifferenzierung ist per se weder verboten noch grundsätzlich illegitim. Sie ist ein wesentlicher Bestandteil gesunden Wettbewerbs, auch in der Finanzwirtschaft. Ähnlich wie bei dem oben beschriebenen Phänomen der auf Basis von BDAI perfektionierten Risikoadäquanz wird eine im Wettbewerb eingesetzte, nach Kundensegmenten, Geographien oder Lebenssituationen differenzierende Preisstrategie allerdings fragwürdig, wenn sie dank BDAI extreme Asymmetrien erzeugt. Einfacher ausgedrückt: Wie groß darf die Waffenungleichheit zwischen dem allwissenden Produktanbieter und dem vollständig gläsernen und buchstäblich ausrechenbaren Kunden werden, bevor Gesellschaften beginnen, sich zu wehren, und Gesetzgeber und, im Falle von Finanzdienstleistern, Regulierer einschreiten? Es wird notwendig sein, solche schwierigen Diskussionen zu führen und Abwägungen vorzunehmen. Finanzregulierung findet seit Jahrzehnten in solchen Zyklen statt. Die Industrie wäre gut beraten, sie zu antizipieren.

12 Unter Konsumentenrente versteht man die Differenz zwischen dem Preis, den ein Verbraucher für ein Produkt oder eine Dienstleistung maximal zu zahlen bereit ist, und dem Preis, den er tatsächlich am Markt zahlen muss.



3.3.1 Bewusste Diskriminierung

Über die Verknüpfung von Informationen aus verschiedenen Quellen lässt sich mit Hilfe von BDAI also relativ präzise die Zahlungsbereitschaft und -fähigkeit für konkrete Produkte und Dienstleistungen offenlegen. Ein Spezifikum von BDAI-Anwendungen besteht zudem darin, dass auch Merkmale, die nicht direkt erhoben werden, offengelegt werden können. Vereinfacht formuliert, muss die zehnte Eigenschaft eines Kunden nicht mehr erhoben werden, wenn sie sich aus neun anderen Eigenschaften sehr sicher schließen lässt. Kommt es zu einer Diskriminierung, können Verbraucher diese dann nicht einmal mit den persönlichen Daten in Verbindung bringen, die sie freigegeben haben. Sie können gegen diese Diskriminierung also auch nicht vorgehen. Die Unternehmen müssen auf eine solche Diskriminierung verzichten und dies für Außenstehende wie zum Beispiel Aufsichtsbehörden überprüfbar machen. Entscheidungen auf der Grundlage von Algorithmen müssen erklärbar sein. Nur so kann eine Unternehmensstruktur und -kultur etabliert werden, die Diskriminierung wirksam verhindern kann.

3.3.2 Unbewusste Diskriminierung

Selbst wenn das Unternehmen beziehungsweise der Softwarenentwickler keine bösen Absichten hatte, kann es sein, dass sich ein Algorithmus diskriminierend verhält beziehungsweise diskriminierende Entscheidungen trifft. Der Algorithmus lernt aus Daten. Suggerieren diese Daten ihm ein diskriminierendes Weltbild oder legen sie zur Erreichung der optimalen Lösung, also der Gewinnmaximierung, diskriminierende Entscheidungen nahe, so kann es passieren, dass Personen(-gruppen)

© iStock/from2015

unbewusst diskriminiert werden. Für die Lösung dieses Problems gibt es technische Ansätze, zum Beispiel Verfahren der nichtdiskriminierenden Datenanalyse und -auswertung. Bei diesen Verfahren muss die anspruchsvolle Hürde genommen werden, den ethischen/rechtlichen Begriff der Diskriminierung in eine mathematische Definition zu überführen, damit die Diskriminierung algorithmisch überprüft und verhindert werden kann. Zurzeit gibt es viele Ansätze und Forschungsprojekte zu diesem Thema, ein von der Wissenschaft allgemein akzeptierter Standard existiert aber bislang nicht. Letztendlich müssen aber die Unternehmen sicherstellen, dass Algorithmen so konzipiert werden, dass rechtliche Rahmenbedingungen berücksichtigt werden. Sie müssen mit hinreichenden Kontroll- und Transparenzmechanismen vermeiden, dass fehlerhafte oder unzulässige Schlussfolgerungen aus ihren Modellen gezogen werden.

4 Zusammenfassung

BDAI hat das Potenzial, die Finanzmärkte tiefgreifend zu verändern. Die neuen Verfahren können zu einem entscheidenden Wettbewerbsvorteil werden. Unternehmen werden daher kaum daran vorbeikommen, eine Strategie für den Umgang mit BDAI zu entwickeln: Sicher werden viele in BDAI-Readiness investieren, also sich und ihre Systeme BDAI-fit machen. Vielleicht wird es aber auch Unternehmen geben, die ihre Nische darin finden, Produkte und Dienstleistungen mit dem Label „garantiert BDAI-frei" anzubieten.

Auch Aufsicht und Regulierung haben noch keine fertigen Antworten auf alle Fragen, die das Phänomen BDAI stellt. Genau aus diesem Grund hat die BaFin im Juni 2018 ihren Bericht zu BDAI veröffentlicht. Auf dieser Basis will sie einen offenen Dialog führen – mit der Industrie, mit der internationalen regulatorischen Gemeinschaft, mit der Wissenschaft und mit der Presse (siehe Infokasten „Konsultation").

Konsultation

Der Bericht „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen" soll die Grundlage für einen intensiven Austausch über den Themenkomplex *Big Data* und künstliche Intelligenz schaffen. Die BaFin hat daher unter anderem Unternehmen und Verbände, andere nationale und internationale Aufsichtsbehörden, Vertreter der Wissenschaft und Journalisten, aber auch Verbraucher zu einer Konsultation ihres Berichts eingeladen. Nähere Informationen finden sich auf www.bafin.de.

Die eingereichten Stellungnahmen werden nicht einzeln veröffentlicht. Die BaFin beabsichtigt aber, eine anonymisierte und aggregierte Auswertung im Internet zu veröffentlichen.

Auch die nächste Ausgabe der BaFinPerspektiven wird sich mit der Auswertung befassen. Ihre Stellungnahme können Sie bis zum 30. September 2018 unter Nennung Ihres Namens, Ihrer Institution sowie Ihrer Adresse an Konsultation.BDAI@bafin.de senden.

II

Die Finanzwelt durchlebt – bedingt durch die Auswirkungen von *Big Data Artificial Intelligence* (BDAI) – einen tiefgreifenden Wandel. Etablierte Banken werden sich vor allem dann behaupten, wenn sie konsequent an ihren Stärken arbeiten, ihre Vorort-Präsenz nutzen und Kunden einen echten Mehrwert bieten.

„Diese Verdrängungsdebatte ist mir zu oberflächlich."

Interview mit

Prof. Dr. Stephan Paul,
Inhaber, Lehrstuhl für Finanzierung und Kreditwirtschaft Ruhr-Universität Bochum


© privat

Herr Professor Paul, Bill Gates prophezeite 1994, „banking is necessary, banks are not". Muss man 2018 sagen, dass er Recht hatte? Wird sich seine Vorhersage in den nächsten Jahren erfüllen?
Mit Verlaub, aber diese Verdrängungsdebatte war und ist mir zu oberflächlich. Was wir erleben, sind doch Metamorphosen, Wandlungsprozesse, wie sie bereits in anderen Branchen zu beobachten waren. Beispielsweise hat man auch Büchern und Zeitungen vor zwei Jahrzehnten das Aus prophezeit. Sie existieren trotz aller wirtschaftlichen Probleme immer noch, haben sich unter dem Druck der Digitalisierung aber gewandelt. So auch in der Kreditwirtschaft: Banken haben ihre in- und externen Prozesse schon erheblich angepasst, müssen aber noch eine lange Wegstrecke gehen, um zukunftsfähig zu bleiben. Meine Prognose lautet daher: Banken wird es auch in 25 Jahren noch geben, sie sehen nur vollkommen anders aus als heute.

Welche Technologie halten Sie auf dem Weg in die Zukunft der Banken für den entscheidenden Game-Changer?
Die Auswertung sehr großer Datenmengen mit Hilfe künstlicher Intelligenz – *Big Data Artificial Intelligence* (BDAI) – hat sicherlich die gravierendsten Auswirkungen. So sieht man zum Beispiel im Bereich der Vermögensberatung – deren Ausbau sich ja viele Banken angesichts schwacher Zinserträge auf die Fahnen geschrieben haben –, dass das auf BDAI basierende *Robo Advisory* für einen Grundbedarf des privaten Portfolio-Managements eine sehr effektive und zudem effiziente Lösung sein kann. In diesem Bereich wird die persönliche Beratung sowohl aus Kosten- als auch Qualitätsgründen zunehmend zur zweitbesten Alternative. Noch stärker werden wohl die internen Prozesse der Banken durch BDAI revolutioniert, nehmen Sie nur als Beispiel die Bonitätsprüfungen im Kreditgeschäft.

Was ist mit der Blockchain-Technologie?
Dort sehen wir erste Anbieter, die auf dieser Technologie ihr Geschäftsmodell aufbauen, quasi „Fintech 2.0". Speziell unter dem Sicherheitsaspekt handelt es sich fraglos um eine Technologie mit Zukunftspotenzial. Wenn ich mir allerdings ansehe, wie viel Energie die *Blockchain* verbraucht und wie zeitaufwändig die Transaktionen sind, scheint mir die derzeitige Euphorie übertrieben. Dagegen ist BDAI-Kompetenz schon heute entscheidend, wenn man Wettbewerbsvorteile erzielen will.

Und hier muss die Kreditwirtschaft aufpassen, gegenüber den Datenriesen aus anderen Branchen nicht ins Hintertreffen zu geraten.

Etablierte Banken und Versicherer versuchen, in eigenen Labs mit agilen Methoden Fintechs beziehungsweise Insuretechs zu kopieren. Glauben Sie, dass es ihnen gelingen wird, den technologischen Vorsprung aufzuholen und am Markt zu bleiben?
Diese Labs schießen ja derzeit wie Pilze aus dem Boden. Doch mit ihrer Einrichtung allein ist es nicht getan. Ausschlaggebend ist, wie die Impulse aus solchen Denkfabriken in die bestehende Organisation hineinwirken und tradierte Unternehmenskulturen verändern. Das Lab darf keine isolierte Insel sein. Es müssen möglichst viele Brücken zum Festland geschlagen werden, damit es zum Innovationstreiber der Organisation werden kann. Selbst dann wird es aber nicht jeder Bank gelingen, an die Spitze des Digitalisierungstrends zu kommen. Das wäre auch zu unwirtschaftlich. Stattdessen wird es, was sich heute schon zeigt, immer mehr Kooperationen zwischen Banken und Versicherern auf der einen und Fintechs/Insurtechs auf der anderen Seite geben. Die Etablierten und die Neuen werden sich gegenseitig befruchten und verändern – im Sinne von Metamorphosen.

Die Digitalisierung von Geschäftsmodellen setzt zunächst eine Standardisierung von Daten und Prozessen voraus. Diese Standardisierung bringt naturgemäß auch Einbußen bei der Flexibilität mit sich.

Wie kritisch sehen Sie diesen Verlust an Flexibilität für den Gesamtmarkt und gibt es hierzu bereits erste Lösungsansätze?
Was die Basisbedarfe sowohl im Privat- als auch im Firmenkundengeschäft angeht, hat die Standardisierung ja schon weit um sich gegriffen, und die Digitalisierung beschleunigt diesen Trend in der Tat. Hier kann nicht mehr jede Bank ihren eigenen Weg wählen. Gleichartige Produktangebote, basierend auf ebenso gleichartigen IT- und Steuerungssystemen, unter Umständen bezogen bei nur wenigen Lieferanten, bergen aber die Gefahr einer Homogenisierung in sich, die in letzter Konsequenz auch ein Systemrisiko darstellt. Da sich dieser Trend aber wohl nicht mehr umkehren lässt, ist für mich die Frage umso bedeutender, wo die jeweilige Bank künftig noch ihre Individualität wahren und dem Kunden Kompetenz und Relevanz demonstrieren kann, denn nur damit lassen sich nachhaltige Wettbewerbsvorteile erzielen.

Und wo könnte das sein?
Im Firmenkundengeschäft ganz klar in der Begleitung und Beratung der Kunden bei der Weiterentwicklung ihrer Geschäftsmodelle in der digitalisierten Industrie-4.0-Welt. Wir erleben in nahezu allen Branchen den stärksten Umbruchprozess seit Jahrzehnten. Was dieser aber für die Unternehmensfinanzierung bedeutet, ist noch gar nicht richtig durchdacht. Wenn die Praxis-Formel „die Finanzierung muss zum Geschäftsmodell passen" zutrifft, dann stehen mit der Disruption von Geschäftsmodellen und neuartigen Formen der Organisation und Steuerung von Wertschöpfungsketten auch die Anforderungen an die Finanzleiter der Unternehmen in Bezug auf die Liquiditätsbeschaffung vor radikalen Veränderungen.

Die Intensivierung der unternehmensübergreifenden Kooperationen von Wertschöpfungspartnern wirft zum Beispiel die Frage auf, worauf sich die Bonitätseinschätzung im Rahmen des Bankenratings künftig idealerweise beziehen soll. Die klassische Unternehmensfinanzierung wird nämlich immer mehr zu einer – vom Gesamtunternehmen losgelösten – Projektfinanzierung. Der Einzelwandelt sich zum Value-Chain-Kredit. Damit sind größere Investitionen gemeint, die zunehmend im Netzwerk mehrerer Unternehmen über verschiedene Wertschöpfungsstufen hinweg getätigt werden und deren Gelingen von der Qualität der beteiligten Partner abhängt. Für den Erfolg des Projekts und damit die Fähigkeit zur Zahlung der Kreditverpflichtungen ist damit nicht mehr nur ein einzelner Akteur verantwortlich, sondern das Geflecht der Akteure – mit zum Teil unterschiedlichen Bonitäten. Auch bei Sicherheiten, die Kreditverträgen zumindest im Mittelstand vielfach noch zugrunde liegen, führt Industrie 4.0 zu Veränderungen: Unternehmensinvestitionen werden im Zuge der Digitalisierung weniger durch klassisches Anlagevermögen geprägt, sondern immer mehr durch immaterielle *Assets* wie insbesondere Software und Patente (*Intellectual Property*), aber auch durch Betreuungs-, Pflege- und Ausbildungsaufwand. Diese immateriellen *Assets* sind in vielen Fällen so unternehmensspezifisch, dass sich die Berechnung von Beleihungswerten und -grenzen kaum auf allgemein akzeptierte Marktpreise stützen kann, wie wir es bei Rohstoffen, Fahrzeugen oder selbst Immobilien kennen.

Kunden in diesem Umbruchprozess zu beraten, ist für die Banken eine große Chance, setzt aber voraus, dass die Firmenkundenberater kräftig an Kompetenz zulegen.

Wie sieht es im Privatkundengeschäft aus?
Die Mehrheit der Generation Z, also der Kunden von morgen, gibt selbstkritisch an, dass ihre ökonomische Allgemeinbildung nicht ausreicht, um sich ohne Hilfe eine angemessene Altersvorsorge aufzubauen. Gerade weil nach empirischen Untersuchungen auch Jüngere den persönlichen Ansprechpartner schätzen, ergibt sich hieraus eine große Chance für Banken. Der personalisierte Flächenvertrieb erweist sich als wichtige Stärke, macht Nähe sachlich und emotional erlebbar. Allerdings steigen auch hierdurch die Anforderungen an die Kompetenz deutlich – vor allem, was die Vermögensberatung angeht. Wettbewerbsvorteile gegenüber den Fintechs werden sich nur dann erzielen lassen, wenn der Berater auch einem zunehmend verbesserten *Robo Advisory* überlegen ist. Daher hat der persönliche Vertrieb vor Ort Zukunft, aber an weniger Standorten und mit höher qualifiziertem Personal.

Herr Professor Paul, wir danken Ihnen für das Interview!

III

Die *Blockchain* stellt eine zusätzliche logische Schicht auf dem Internet bereit, um Werte zu transportieren. Die Lernkurve ist steil, aber durch *Blockchain* kann IT sowohl sicherer als auch massiv günstiger werden.

Distributed-Ledger-Technologie: Die Blockchain als Basis für IT-Sicherheit

Autoren

Christian Flasshoff,
Wiss. Mitarbeiter, Frankfurt School Blockchain Center, Frankfurt am Main

Michael Mertens,
Vorstandsvorsitzender, CryptoTec AG, Köln

Prof. Dr. Philipp Sandner,
Leiter, Frankfurt School Blockchain Center, Frankfurt am Main

Sebastian Stommel,
Research, CryptoTec AG, Köln

1 Einleitung

Die Blockchain-Technologie hat seit der Einführung des Bitcoins im Jahr 2008 zunehmende Bekanntheit erlangt. Die *Blockchain* kann jedoch weitaus mehr, als eine digitale Währung zu verwalten. Die Technologie hat das Potenzial, etablierte Geschäftsmodelle grundlegend in Frage zu stellen. Die Erwartungen an die Blockchain-Technologie werden schon dadurch deutlich, dass die Marktkapitalisierung der so genannten Kryptowährungen 2017 auf über 600 Milliarden US-Dollar gestiegen ist.[1] Im vierten Quartal 2017 überstiegen die durch *Initial Coin Offerings* (ICOs) erzielten Investorengelder herkömmliche Venture-Capital-Finanzierungen um das 16-fache.[2] Ein ICO ist vergleichbar mit einem Börsengang, bei dem Geld von Investoren eingesammelt wird, basiert jedoch auf der Blockchain-Technologie.

Um eine Bewertungshilfe für das realistische Potenzial der Blockchain-Technologie bereitzustellen, wird in diesem Artikel die Blockchain-Technologie im Vergleich zu herkömmlichen IT-Systemen näher beleuchtet. Ein besonderer Fokus liegt dabei auf der Sicherheit von IT-Systemen. Die Blockchain-Technologie stellt viele Grundsätze herkömmlicher IT in Frage und löst viele Sicherheitsfragen grundlegend anders. Die *Blockchain* hat dabei das Potenzial, die Sicherheit von IT-Systemen erheblich zu erhöhen und zugleich die IT-Kosten massiv zu reduzieren. Die *Blockchain* ist nicht automatisch die beste Lösung für jedes Problem. Bei der Umsetzung sind überdies besondere Anforderungen zu beachten, um Risiken vorzubeugen. Daher werden im Artikel auch kritische Faktoren für die erfolgreiche Umsetzung von Blockchain-Projekten beschrieben. Um die bestmögliche Sicherheit von Blockchain-Anwendungen zu gewährleisten, ist es geboten, Kryptografie-Experten früh in den Entwicklungsprozess einzubeziehen. Die *Blockchain* verändert nicht nur die IT-Abteilung eines Unternehmens, sondern kann Einfluss auf die Struktur der gesamten Wertschöpfungskette nehmen. Daher wird das Veränderungspotenzial von Geschäftsprozessen in Unternehmen auch aus einer holistischen Perspektive betrachtet.

1 Coindesk, Q4 2017 State of Blockchain, https://www.coindesk.com/research/state-blockchain-q4-2017, abgerufen am 08.05.2018.
2 Coindesk, a.a.O. (Fn. 1).

2 Vorteile der Blockchain-Technologie

2.1 Unveränderbare Datenbank

Die *Blockchain* ist eine unveränderbare, sich kontinuierlich weiter entwickelnde Datenbank (*Ledger*). In der Unveränderbarkeit liegt ein Vorteil gegenüber konventionellen Datenbanken, der in der Regel unterschätzt wird. Zurzeit sind Daten sehr leicht zu verändernde Objekte. So ist es beispielsweise nicht schwierig, einen Eintrag im Hauptspeicher eines Computers oder einer konventionellen Datenbank zu verändern. IT-Systeme sind sogar darauf ausgelegt, dass Daten nachträglich leicht zu verändern sind. Diese Funktion ist für viele Anwendungsfälle sinnvoll, jedoch wird dadurch die Sicherheit bei konventionellen IT-Systemen auch stark gefährdet. Die Blockchain-Technologie führt hierbei zu einem Paradigmenwechsel, indem die vollkommene Unveränderbarkeit von Daten komplett neue Ansätze beim Aufbau von IT-Systemen ermöglicht. So ist es nicht mehr notwendig, die Sicherheit von Systemen mittels dedizierter Infrastruktur und *Firewalls* aufwendig zu schützen. Vielmehr sind in der *Blockchain* alle Daten bereits mittels Kryptografie gesichert und können nicht manipuliert werden.

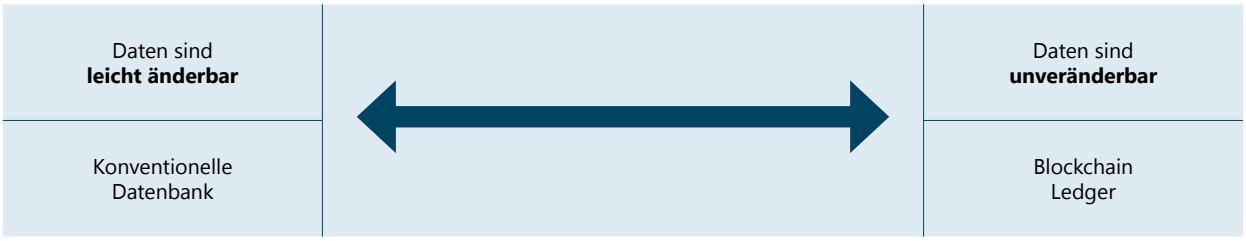
Diese Unveränderbarkeit von Daten ermöglicht die Umsetzung komplett neuer Geschäftsmodelle, weil die auf der *Blockchain* abgespeicherten Daten belastbar und vertrauenswürdig sind. Folglich können beispielsweise Bezahlvorgänge auf Grundlage dieser Daten automatisch ausgeführt werden, und der Intermediär, der die Echtheit der Daten bestätigt oder garantiert, wird überflüssig. Die Daten auf einer *Blockchain* sind so sicher, dass sogar Besitz- und Eigentumsverhältnisse, wie es in einem Grundbuch der Fall ist, sicher darauf abgelegt werden können. Selbst demokratische Wahlen können durch eine *Blockchain* manipulationssicher durchgeführt werden. Es ist bei gleichzeitiger Bewahrung des Wahlgeheimnisses dabei für jeden nachvollziehbar, dass die Wahlen korrekt abgelaufen sind

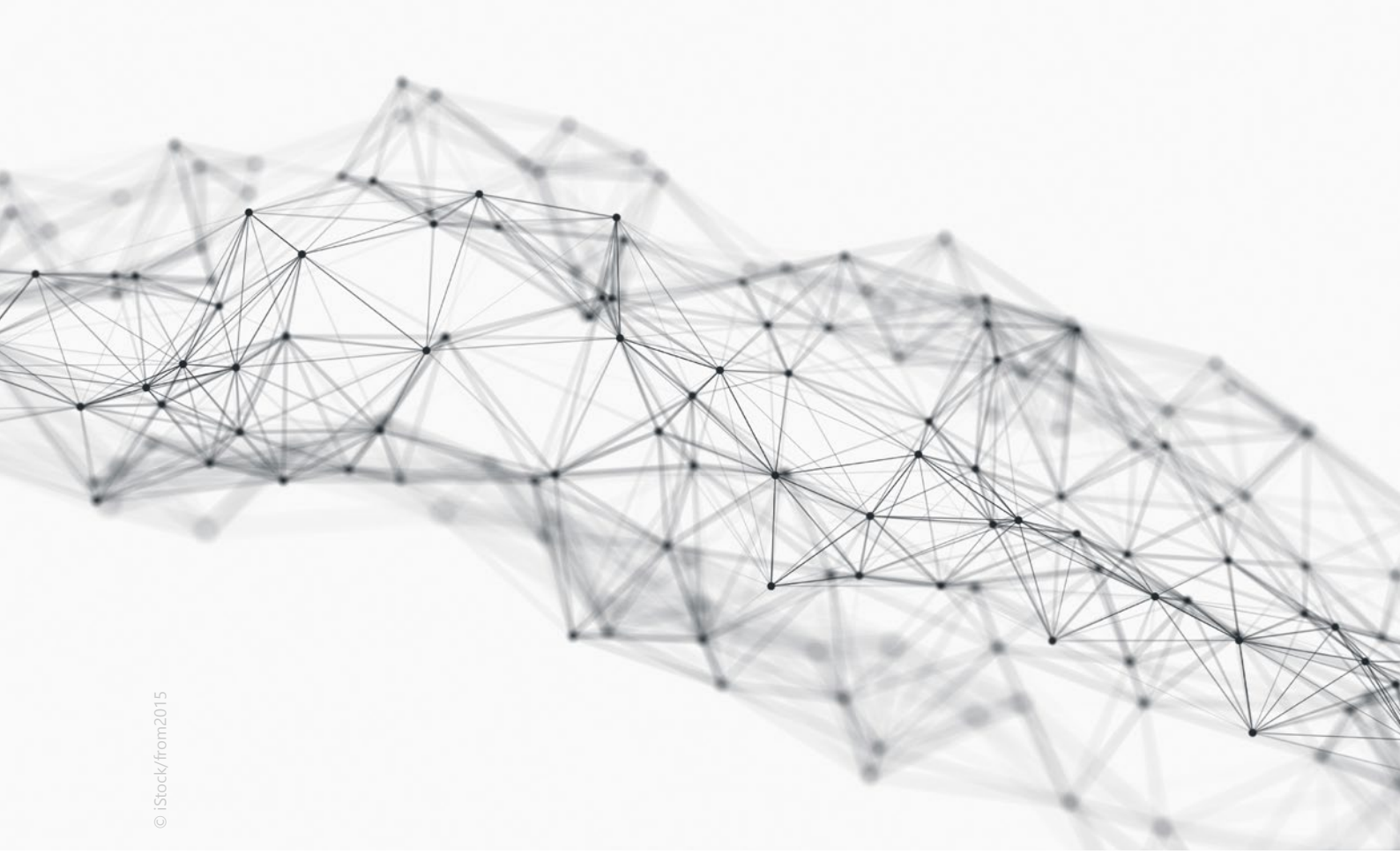
2.2 Trustless Systems

Bislang galt der Grundsatz: Je länger Daten im System sind, desto unsicherer werden sie, da Angreifer die Daten manipulieren konnten. Die Zeitdauer zwischen erfolgreichem Angriff und Entdeckung des Angriffs beträgt im Durschnitt 180 Tage.[3] Die *Blockchain* dreht diesen Grundsatz vollständig um: Je länger Daten in der *Blockchain* sind, desto sicherer werden sie, da die Echtheit von Daten von immer mehr Teilnehmern im Netzwerk bestätigt wird. Für die Sicherheit einiger Blockchain-Architekturen ist es sogar unwesentlich, ob die Identität der Teilnehmer bekannt oder unbekannt ist. Früher wurden Systeme beim Zugriff durch unbekannte Teilnehmer zunehmend unsicherer. Mit einer *Blockchain* können auch unbekannte Teilnehmer interagieren und das System sicherer machen.

3 Backofen, Wir brauchen die flächendeckende Immunisierung der Gesellschaft gegen Cyberattacken!, https://www.telekom.com/de/konzern/management-zur-sache/details/immunisierung-der-gesellschaft-gegen-cyberattacken-517376, abgerufen am 08.05.2018.

Abbildung 1: Konventionelle Datenbank vs. Blockchain Ledger





Die Bezeichnung „*Trustless System*" bedeutet im Zusammenhang mit der *Blockchain*, dass den beteiligten Servern und deren Betreibern nicht vertraut werden muss, da die Daten auf der *Blockchain* nachweisbar nicht manipuliert werden können. Die *Blockchain* selbst erzeugt Vertrauen im System, da die Blockchain-Protokolle automatisch prüfen, ob die Regeln der *Blockchain* von den Teilnehmern eingehalten werden. Prozessrisiken können so reduziert werden, indem eine *Blockchain* automatisch sicherstellt, dass Verträge ausgeführt und Zahlungen durchgeführt werden.

2.3 Schutz vor Datendiebstahl

Ein weiterer Vorteil der Blockchain-Technologie gegenüber konventionellen Datenbanken liegt im Schutz vor dem Diebstahl riesiger Datensätze. In der Vergangenheit gab es häufig Schlagzeilen zu Hacks zentraler Datenbanken mit Millionen von gestohlenen Datensätzen wie bei Sony, Target und Home Depot. Da eine *Blockchain* etwa Kreditkarten-Datensätze nicht mehr benötigt, sondern auf Ende-zu-Ende-Sicherheit setzt, können die Daten auch nicht mehr von Servern gestohlen werden. Insbesondere bietet die Blockchain-Technologie aber auch die Möglichkeit, Daten verschlüsselt abzulegen. Zudem können auf *Blockchains* durch internationalen Konsens direkte Zahlfunktionalitäten und automatisch ausführende Verträge (*Smart Contracts*) implementiert werden. Solche und viele weitere Möglichkeiten gehen weit über die Funktionalität herkömmlicher Datenbanken hinaus.

2.4 Transparenz und Verifizierbarkeit

Eine weitere Innovation durch die *Blockchain* ist die Validierung von gespeicherten Daten. Die Informationsbeschaffung ist im Zeitalter des Internets sehr einfach geworden. Das Wertversprechen von Google ist, alle verfügbaren Daten auf der Welt durch ein einziges Suchmaschinen-Fenster auffindbar zu machen. Eine Validierung der Daten ist oft jedoch nur schwer möglich. Die Blockchain-Technologie ermöglicht es nun, dass die Echtheit aller Daten auf der *Blockchain* geprüft werden kann. Diese Eigenschaft bringt viele Anwendungsmöglichkeiten mit sich. So können Kunden beispielsweise sicher davon ausgehen, dass Medikamente auf Basis von echten klinischen Studien entwickelt wurden, dass Autos anhand valider Studien von Abgaswerten entwickelt wurden und dass Nahrungsmittel wirklich in den angegebenen Regionen hergestellt worden sind. Die Validierung der Daten auf der *Blockchain* erhöht so die Transparenz für Unternehmen, Kunden und Bürger.

3 IT-Sicherheit durch die Blockchain

IT-Sicherheit ist in vielen Unternehmen ein wichtiges Ziel. Im Allianz Risk Barometer 2018 wird die Gefahr von Cyberattacken als zweitgrößtes Risiko für Unternehmen in Deutschland aufgeführt.[4] Die Auswirkungen von Cyberattacken musste beispielsweise der Logistikdienstleister Maersk erfahren. Durch einen Angriff des Trojaners Not-Petya ist schätzungsweise ein Schaden von 200 bis 300 Millionen US-Dollar entstanden.[5] Neben erhöhten Sicherheitsanforderungen in der IT verfolgen Unternehmen zugleich das Ziel, Kosten für IT-Bestandssysteme zu senken und die Interoperabilität zu erhöhen. Die *Blockchain* kann hierbei eine Schlüsseltechnologie sein und Unternehmen dabei helfen, die IT-Sicherheit zu erhöhen und die Kosten zu senken. Gegenüber den typischen Angriffen auf Webanwendungen[6] sind *Blockchains* deutlich resistenter.

3.1 Trennung der Informations- und Netzwerksicherheit

Was genau macht Blockchain-Anwendungen im Vergleich zu herkömmlichen IT-Systemen so sicher? Um diese Frage beantworten zu können, ist es notwendig, sich mit dem Aufbau der Netzwerksicherheit herkömmlicher IT-Systeme zu beschäftigen. Herkömmliche IT-Systeme sind durch eine strikte Trennung zwischen außen und innen gekennzeichnet. Nur Teilnehmer im Inneren des Systems haben Zugriff auf die Daten und können Änderungen im System vornehmen. Um Sicherheit zu gewährleisten, erfolgt eine Zugangskontrolle zum inneren Teil auf der Betriebssystemebene.

Abhängig vom erforderlichen Sicherheitslevel ist diese Zugangskontrolle aufwändiger und oder weniger aufwändig konzipiert. Die Sicherheit herkömmlicher IT-Systeme wird beispielsweise durch *Firewalls* und verschlüsselte VPN[7]-Verbindungen gewährleistet.

In der Welt der *Blockchains* wird hingegen diese Trennung von innen und außen beinahe aufgehoben. Bei einer *Public Blockchain* handelt es sich um eine öffentliche und redundant gespeicherte Datenbank. Die Sicherheit der Daten hängt nur am Besitz des jeweiligen Schlüssels und wird durch kryptografische Protokolle gewährleistet. Die Sicherheit braucht daher nicht durch *Firewalls* gewährleistet zu werden. Die *Blockchain* entkoppelt damit die Informationssicherheit von der Netzwerksicherheit. Es ist im Grunde genommen egal, ob Fremde Zugriff auf die *Blockchain* haben (Netzwerksicherheit), solange die Daten auf der *Blockchain* durch Kryptografie geschützt sind (Informationssicherheit). Selbstverständlich muss eine *Blockchain* nicht zwingend öffentlich zugänglich sein, sondern kann auch innerhalb eines Unternehmens verbleiben (*Private Blockchain*). Dieser Blockchain-Ansatz ermöglicht eine erhöhte Sicherheit von Daten und reduziert zugleich den benötigten Sicherheitsaufwand im Vergleich zu herkömmlichen IT-Systemen.

3.2 Sicherheit von Blockchain-Standards

Die Blockchain-Technologie befindet sich noch am Anfang der Entwicklung. Daher gibt es viele unterschiedliche Anbieter mit verschiedenen Lösungsansätzen. Oft wird bemängelt, dass die *Blockchain* noch keine ausreichenden und einheitlichen Standards besitze.[8] Es werden jedoch selten Wettbewerbsvorteile durch die Erfüllung von Standards erzielt, sondern vielmehr durch das Setzen von Standards. Unternehmen wie Microsoft,

4 Allianz Risk Barometer, Die 10 wichtigsten Geschäftsrisiken in Deutschland, https://www.allianz.com/v_1516057200000/media/press/photo/risk-barometer-2018/Allianz_Risk_Barometer_2018_Top_10_Business_Risks_Deutschland.jpg, abgerufen am 08.05.2018.

5 Scherschel, Heise Online – NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust, https://www.heise.de/newsticker/meldung/NotPetya-Maersk-erwartet-bis-zu-300-Millionen-Dollar-Verlust-3804688.html, abgerufen am 08.05.2018.

6 OWASP, Top 10 – 2017, The Ten Most Critical Web Application Security Risks, https://www.owasp.org/index.php/Top_10-2017_Top_10, abgerufen am 08.05.2018.

7 Virtual Private Network.

8 Hasso Plattner Institut, Bitcoin-Hype: HPI-Studie zum echten Innovationspotenzial der Blockchain, https://hpi.de/pressemitteilungen/2018/bitcoin-hype-hpi-studie-zum-echten-innovationspotenzial-der-blockchain.html, abgerufen am 08.05.2018.

Apple, Google und Facebook gehören zu den wertvollsten Unternehmen der Welt, gerade weil sie eigene Standards gesetzt haben und nicht erst auf andere Standards gewartet haben. Für Wettbewerbsvorteile bei neuen Technologien ist es oft wichtiger, schneller im Markt zu sein, als die perfektere Technologie zu bieten. Gerade bei der *Blockchain* kann aber auf Sicherheit nicht verzichtet werden. Vor allem wenn wenig bestehende Technologie wiederverwendet und alles neu entwickelt wird, enthalten Blockchain-Entwicklungen oft kritische Implementierungsfehler. So wurde beispielsweise zCoin Opfer eines Denial-Of-Spending-Angriffs. Hierbei wurde ein Fehler im Protokoll ausgenutzt, und Angreifer konnten über *Coins* verfügen, die ihnen nicht gehörten.[9] Auch der DAO-Hack[10] ist ein bekannter Fall. Bei der Umsetzung von Blockchain-Projekten ist es daher von zentraler Bedeutung, dass das Projektteam mit Kryptografie-Experten zusammenarbeitet. Nach Möglichkeit sollte begleitend zur Implementierung ein formaler Sicherheitsbeweis erarbeitet werden. Auf diesen Aspekt wird in Abschnitt 5.1 detaillierter eingegangen.

3.3 Kommunizierbare Mehrwerte

Die Blockchain-Technologie bringt signifikante Vorteile für die IT-Sicherheit mit sich. Dies bedeutet jedoch nicht, dass die *Blockchain* automatisch für alle Anwendungsfälle die beste Technologie ist. Bevor man sich in einem Unternehmen dafür entscheidet, eine blockchainbasierte Lösung zu implementieren, ist eine genaue Analyse der Mehrwerte erforderlich. Ansonsten besteht die Gefahr, dass Blockchain-Anwendungen programmiert werden, die im Vergleich zu anderen IT-Lösungen keine wirklichen Vorteile haben. Hierbei ist der Grundsatz der Kommunizierbarkeit hilfreich. Mehrwerte müssen dem Kunden oder anderen Stakeholdern gegenüber verständlich kommuniziert werden können. Blockchain-Anwendungen, die diesen Grundsatz erfüllen, rechtfertigen die Investition und tragen zum Unternehmenserfolg bei. Ist dies nicht der Fall, so ist *Blockchain* möglicherweise nicht die beste verfügbare Technologie. In der Folge werden einige Beispiele für einen tatsächlichen Sicherheitsmehrwert durch die Blockchain-Technologie dargestellt:

- Zahlungen in einem Peer-to-peer-Blockchain-Netzwerk sind sicher validiert und nicht veränderbar. Ein Rückruf, wie es im SEPA-Basislastschriftverfahren möglich ist, ist ausgeschlossen.
- Die Verwaltung von Nutzerdaten über eine *Blockchain* ermöglicht es dem Nutzer, selbst seine digitale Identität zu verwalten und selbst zu entscheiden, welcher Anbieter Zugriff auf welche Daten erhalten soll. So kann ein Nutzer von der Verwendung seiner Daten unmittelbar selbst profitieren, zum Beispiel durch die Überlassung im Rahmen einer klinischen Studie.
- Sobald ein *Smart Contract* von beiden Vertragsparteien digital signiert ist, garantiert der Programmiercode die Erfüllung des Vertrags. Diese Sicherheitsmehrwerte können Kunden und anderen Stakeholdern gegenüber vorteilhaft kommuniziert werden und sind daher gute Anwendungsfälle für die Blockchain-Technologie.

3.4 Kryptografie

Die Kryptografie ist wesentlich für die Sicherheit von Blockchain-Anwendungen. Durch Hash-Verfahren (Rechenoperationen) wird die Integrität von Daten geschützt. Digitale Signaturen schützen die Autorenschaft eines Eintrags. Verschlüsselung schützt den Zugang zu Informationen. Somit ist es möglich, den Zugang und die Verfügung über Daten, Geld, Güter oder andere Werte auf definierte Teilnehmer zu beschränken. Hierfür werden kryptografische Protokolle mit komplexen mathematischen Modellen benötigt. Um zu erläutern, wie die Kryptografie in einer *Blockchain* funktioniert, sind im Folgenden einige Verfahren vereinfacht dargestellt.

9 Schröder, Friedrich-Alexander-Universität Erlangen-Nürnberg – FAU-Forscher warnen vor „verbranntem Geld" bei verschiedenen Kryptowährungen, https://www.fau.de/2018/04/news/wissenschaft/angriff-auf-kryptowaehrung-entdeckt/, abgerufen am 08.05.2018.

10 Biederbeck, WIRED – Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen, https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde, abgerufen am 08.05.2018.

Die Erklärung erfolgt am Beispiel der weit verbreiteten digitalen Währung Bitcoin.

3.4.1 Sichere Identität

Um am Bitcoin-Netzwerk teilnehmen zu können, benötigt jeder Nutzer ein Konto auf der Bitcoin-Blockchain. Hierfür bildet der Computer 256 zufällige Münzwürfe nach und merkt sich das Ergebnis. Es gibt dabei $1.157x10^{77}$ verschiedene Möglichkeiten für das Ergebnis, nämlich

115.792.089.237.316.195.423.570.985.008.687.907.853.
269.984.665.640.564.039.457.584.007.913.129.639.935.

Diese Zahl der Möglichkeiten ist so groß, dass jedem Atom im Universum damit eine eindeutige Nummer zugewiesen werden könnte. Um diese Menge an Möglichkeiten zu generieren, könnte man alternativ 100 Würfel gleichzeitig werfen. Die enorme Zahl der unterschiedlichen Möglichkeiten an Würfelergebnissen ist für die Informationssicherheit auf der *Blockchain* verantwortlich. Ein Erraten des Würfelergebnisses ist unmöglich, und ein Ausprobieren würde selbst mit den leistungsstärksten Computern Millionen von Jahren benötigen. Das Würfelergebnis muss geheim bleiben und dient später als Schlüssel, um die verschlüsselten Informationen lesen zu können. Mit Hilfe von Hash-Verfahren wird aus dem geheimen Würfelergebnis eine öffentliche Bitcoin-Adresse erstellt und auf der *Blockchain* abgelegt. Die Verschlüsselungsverfahren sind öffentlich und können so auditiert werden. Die Sicherheit des Verfahrens beruht auf Kerckhoffs' Maxime aus dem Jahr 1883 und verfolgt den Grundsatz, dass die Sicherheit der Kryptografie auf der Geheimhaltung des Schlüssels basiert statt auf der Geheimhaltung des Verschlüsselungsalgorithmus. Dieser Grundsatz ist ein wichtiger Bestandteil der modernen Kryptografie.

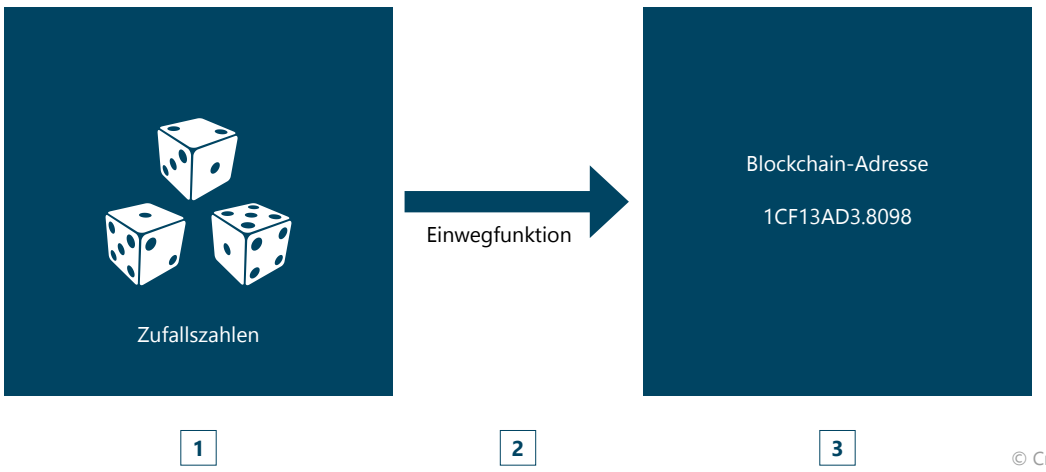
3.4.2 Transaktionen auf der Blockchain

Die zufällig zugewiesene Bitcoin-Adresse repräsentiert ein Konto auf der *Blockchain*. Diese Adresse kann zum Empfangen von Bitcoins verwendet werden. In anderen Blockchain-Netzwerken können auch digitale Güter und sonstige Informationen versendet werden. Eine zufällig erstellte Blockchain-Adresse kann beispielsweise so aussehen:

92024 57150 21345 42342 34121 34230 16215 64644 54627 72316.

Jeder Teilnehmer, der die Adresse kennt, kann digitales Geld oder sonstige Werte an diese Adresse senden, wie

Abbildung 2: Blockchain-Konto und Adresse erzeugen



an die Adresse eines Hauses. Wie bei einem Haus kann nur der Eigentümer der Blockchain-Adresse über das empfangene Geld verfügen oder die empfangene Nachricht entschlüsseln. Die Entschlüsselung erfolgt mit Hilfe des geheimen Schlüssels (Würfelergebnis). Es ist nicht möglich, von einer öffentlichen Blockchain-Adresse auf den zugrunde liegenden geheimen Schlüssel zu schließen. Es handelt sich hierbei um eine Einwegfunktion der asymmetrischen Kryptografie. Einwegfunktionen sind Funktionen, welche einfach berechnet werden können, jedoch in der Umkehrung nicht praktikabel berechenbar sind. So kann aus dem Würfelergebnis eine Blockchain-Adresse berechnet werden, jedoch nicht umgekehrt. Ein Beispiel aus der physikalischen Welt für eine Einwegfunktion ist der Wurf eines Glases auf den Boden. Hierbei zerspringt das Glas in viele kleine Scherben, und es erfordert nicht viel Aufwand, das Glas zu zerstören. Jedoch ist das Zusammensetzen der Scherben zum ursprünglichen Glas nur mit extremem Aufwand möglich.

3.4.3 Authentifizierung der Identitäten

Blockchain-Adressen können jedoch nicht nur als Kontonummern im Bitcoin-Netzwerk verwendet werden. So können beispielsweise Industrieunternehmen einzelnen Produkten, Gütern und Bauteilen individuelle Blockchain-Adressen zuordnen und diese im Produktions- und Distributionsprozess eindeutig identifizieren. Mit Hilfe von QR[11]-Codes können diese Adressen für Maschinen lesbar dargestellt und in einer *Blockchain* registriert werden. Zusätzlich können Blockchain-Adressen beliebige Attribute zugeordnet werden. So erleichtert die Zuordnung des Firmennamens als Attribut anderen Teilnehmern der *Blockchain* die Identifizierung der Adresse. Zum Anheften eines Attributes wird die Kenntnis des Würfelergebnisses benötigt. So kann nachvollzogen werden, dass die Attribute nur von einem Teilnehmer hinzugefügt wurden, der auch Eigentümer der Adresse ist.

In einem Blockchain-Netzwerk ist es jedoch nicht zwingend notwendig, dass man die Teilnehmer des Netzwerkes kennt. Auch unbekannte und nicht bestätigte Teilnehmer können ohne Sicherheitsverlust an der

11 Quick Response (siehe Abbildung 3).

Abbildung 3: QR-Code für eine Blockchain-Adresse

Blockchain teilnehmen. Während unbekannte Teilnehmer in herkömmlichen IT-Systemen ein Sicherheitsrisiko hervorrufen, so ist dies bei öffentlichen *Blockchains* kein Sicherheits- oder Stabilitätsproblem. Diese Eigenschaft ist ein Vorteil der *Blockchain*, da die Hürden für die Hinzunahme von neuen Teilnehmern enorm gesenkt werden und eine kritische Masse an Nutzern schneller erreicht wird. Bitcoin ist hierbei ein sehr gutes Beispiel, da jeder Teilnehmer ein eigenes Konto erzeugen kann, ohne sich vorher bei einer Bank oder Verwaltung registrieren zu müssen. Echtheitsprüfungen der teilnehmenden Identitäten können bei Bedarf später durchgeführt werden. Auch ist es möglich, eine unbekannte Identität später zu verifizieren, so dass auch vorangegangene Aktionen rückwirkend dem bestätigten Teilnehmer zugeordnet werden können. Dieser Vorteil wird auch als *Key Continuity* bezeichnet.

3.5 Identity-Management und Schlüsselverwaltung

Damit Nutzer einer *Blockchain* die langen Zahlen oder die QR-Codes einer Blockchain-Adresse nicht auswendig zu kennen brauchen, gibt es das Blockchain-Identity-Management. Die zugeordneten Attribute (zum Beispiel Firmennamen) geben Auskunft über die Identität des Teilnehmers und können übersichtlich in einer Datenbank abgelegt werden. Das Versenden von Geld an eine Blockchain-Adresse wird damit so einfach wie das Versenden einer E-Mail. Ein kompliziertes Eingeben von langen Kontonummern, wie beispielsweise bei SEPA-Überweisungen, ist bei Blockchain-Anwendungen mit gutem Identity-Management nicht mehr notwendig. Ein gutes Blockchain-Identity-Management

zeichnet sich dadurch aus, dass einer Firma oder einer Person mehrere Blockchain-Adressen zugeordnet werden können. In der Praxis werden nämlich für unterschiedliche Blockchain-Anwendungen verschiedene kryptografische Verfahren verwendet, so dass die Blockchain-Adressen nicht austauschbar sind. So haben beispielsweise Blockchain-Lösungen für einen Dokumentenspeicher andere kryptografische Verfahren als Blockchain-Lösungen für den P2P-Geldtransfer.

Folgendes Beispiel soll dieses Szenario illustrieren: Ein Autor eines Blog-Beitrags wird gewöhnlich für seine erfolgreiche Arbeit bezahlt. Der Beitrag wird allerdings über eine andere *Blockchain* übertragen als die vereinbarte Bezahlung. Das Blockchain-Identity-Management ist die Schnittstelle zwischen beiden *Blockchains* und stellt sicher, dass die Bezahlung an dieselbe Person geht, die auch den Beitrag verfasst hat.

Es wurde bereits die Funktion des Schlüssels (*Private Key*) erläutert. Die Geheimhaltung des Schlüssels ist wichtig, um die Sicherheit der *Wallet* (Konto) und der Daten zu gewährleisten. Der Schlüssel darf auch nicht verloren gehen, da sonst niemand mehr Zugriff auf die digitale *Wallet* oder die gespeicherten Daten hat. Es erfordert daher umfangreiche Backup- und Recovery-Lösungen, sowohl für Privatpersonen als auch für Unternehmen. Selbstverständlich sollten solche Lösungen Ende-zu-Ende verschlüsselt sein, da sonst das Sicherheitsversprechen der *Blockchain* hinfällig ist. Ergänzend können die Schlüssel auch aufgeteilt und redundant bei Treuhändern gespeichert werden. Beispiele für solche Verfahren sind *Shamirs Secret Sharing* und *Multisignature Wallets*.

4 Blockchain in Unternehmen

4.1 Geldfluss, Informationsfluss und Warenfluss

Die *Blockchain* bietet auch in Anwendungen bei Unternehmen viele Vorteile und erlaubt eine schnelle, sichere und kostengünstige Abwicklung von Geschäftsprozessen. Die Technologie ermöglicht eine automatische Abstimmung von Geld-, Informations-, und Warenfluss. In einer *Blockchain* kann jedes Gut, dem ein Wert zugewiesen werden kann, verwaltet werden. Es kann zu jedem Zeitpunkt einwandfrei und verlässlich festgestellt werden, wem das Gut gehört. Des Weiteren kann in einer *Blockchain* Eigentum und Besitz eines Gutes übertragen werden. Eine solche Übertragung von Gütern in der *Blockchain* ist sicher und kann auch nicht ohne Zustimmung des neuen Besitzers rückgängig gemacht werden. Während beim Versand von E-Mails lediglich eine Kopie erzeugt und zwischen den Mailservern ausgetauscht wird, erfolgt auf einer *Blockchain* eine tatsächliche Übertragung des Gutes. Physikalischen Gütern kann ebenfalls ein digitaler *Token* zugeordnet werden, wodurch eine Nachverfolgung des Gutes ermöglicht wird. QR-Codes oder RFID[12]-Chips können dabei helfen, das physikalische Gut und den digitalen *Token* zusammenzuführen.

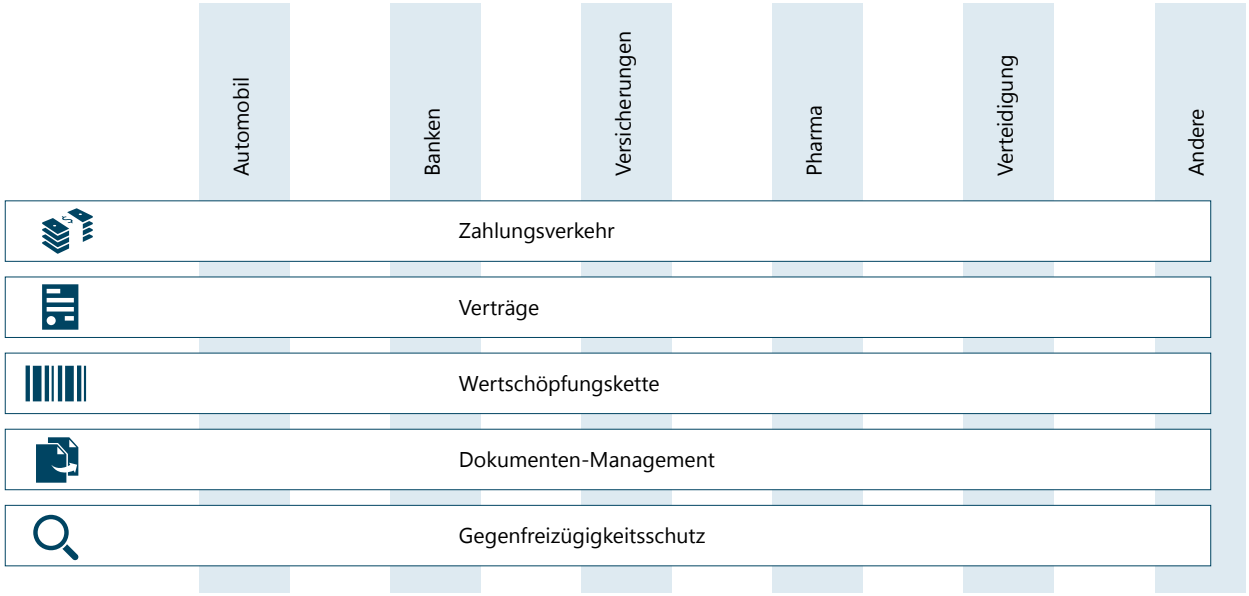
12 Radio-Frequency Identification.

Abbildung 4: Die Blockchain bringt Geldfluss, Informationsfluss und Warenfluss zusammen

4.2 Beschleunigung in der Prozessabstimmung

Eine *Blockchain* kann enorme Effizienzsteigerungen bewirken, indem mehrere Prozesse, wie zum Beispiel Zahlungen, Vertragsschließung, *Supply Chain*, Dokumentenaustausch und Fälschungsschutz, in einem System abgebildet werden. Die *Blockchain* bietet hier die Möglichkeit, Prozessschritte optimal aufeinander abzustimmen. Trifft beispielsweise ein bestelltes Gut bei einem Unternehmen ein, können automatisch Dokumente geprüft und Fälschungen identifiziert werden, der zugrunde liegende Vertrag kann ausgeführt und das Geld an die andere Vertragspartei gesendet werden. Prozesse, die vorher getrennt voneinander abgelaufen sind, können durch die *Blockchain* automatisch und in Sekunden durchgeführt werden. Die erhöhte Durchlaufgeschwindigkeit birgt hohes Potenzial an Kostenreduktion. Die Optimierung von Prozessen durch Blockchain-Lösungen kann Einsparungen von bis zu 99,9 Prozent und eine Beschleunigung um den Faktor 1.000 herbeiführen. Eine horizontale Abstimmung der Prozesskette kann ebenfalls branchenübergreifend verlaufen und weitere Geschäftsprozesse vereinfachen.

Abbildung 5: Horizontale Abstimmung der Prozesskette



4.3 Veränderung der Wertschöpfungskette

Die Blockchain-Technologie ermöglicht direkten Kontakt zu allen Teilnehmern in einer *Supply Chain*. So bekommen Unternehmen, die zurzeit in der Mitte einer *Supply Chain* gefangen sind, die Chance, direkten Kontakt zum Kunden aufzubauen. Hierdurch können Hersteller ein Produkt oder eine Dienstleistung direkt an den Endkunden verkaufen. Diese Chance bedeutet jedoch auch ein Risiko für etablierte Unternehmen, die bisher den exklusiven Marktzugang hatten und zwischen Hersteller und Endkunde vermittelt haben. Die Blockchain-Technologie greift bestehende Geschäftsmodelle an und wertet Zulieferer und Hersteller in der Wertschöpfungskette auf. Zusätzlich können Unternehmen mittels *Blockchain* entlang der Wertschöpfungskette effizienter und schneller miteinander arbeiten. Es ist daher wichtig, die Mehrwerte einer *Blockchain* zu verstehen, um zukünftig zu den Gewinnern zu gehören.

5 Umsetzung von Blockchain-Anwendungen

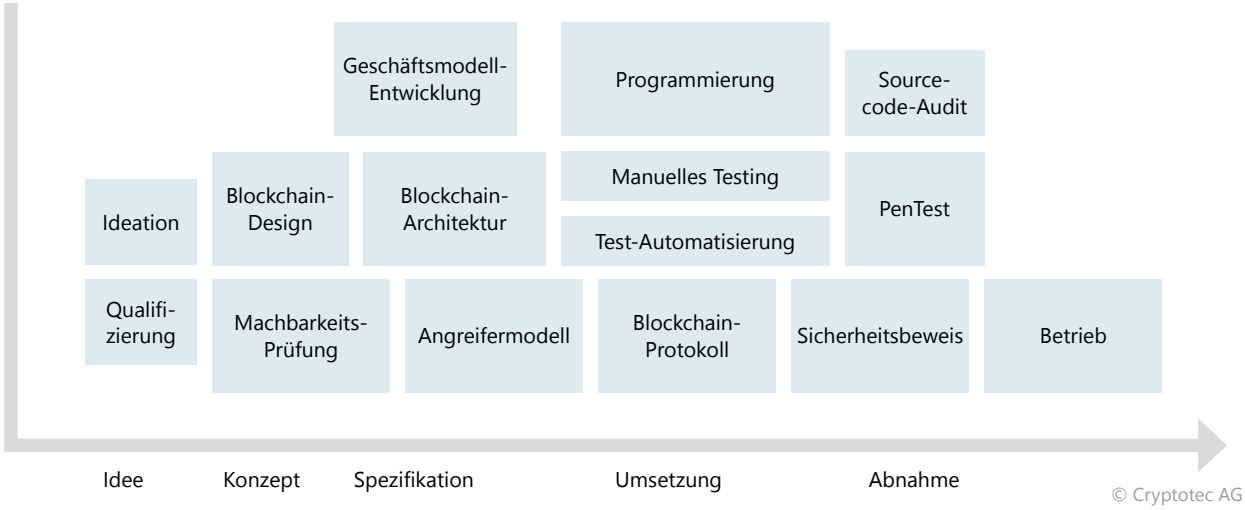
5.1 Sicherheitsbeweis

Die Sicherheit einer Blockchain-Anwendung entscheidet über deren Erfolg oder Misserfolg. Es ist daher wichtig, keine Fehler bei der Entwicklung zu machen, die später die Sicherheit der Anwendung gefährden. Um besser zu verstehen, wie man solche Fehler vermeidet, ist es hilfreich, sich den Prozess der Entwicklung einer Blockchain-Anwendung vor Augen zu führen. Eine Idee für eine *Blockchain* kann in drei Sätzen grob beschrieben werden. Auf circa 40 Seiten lässt sich ein Konzept fixieren. Auf weiteren 150 Seiten werden die Spezifikationen ausgeführt. Die tatsächliche Implementierung kann dann drei Millionen Zeilen Programmcode umfassen und etwa 30.000 Seiten entsprechen.

> „The main advantage of blockchain technology is supposed to be that it‘s more secure, but new technologies are generally hard for people to trust, and this paradox can‘t really be avoided.“
>
> Vitalik Buterin

Nachträglich Millionen Zeilen von Programmcode auf Sicherheit zu prüfen und konzeptionelle Fehler aufzudecken, ist kaum möglich. Konzeptionelle Fehler können jedoch gravierende Folgen für die *Blockchain* haben und in vielen Fällen nicht durch ein Softwareupdate behoben werden. Es ist daher empfehlenswert, früh einen formalen Sicherheitsbeweis zu führen und so gewissermaßen die korrekte Statik des Systems zu gewährleisten. Hier wird mathematisch bewiesen, dass ein System von einem real existierenden Computer nicht gehackt werden kann. Für diesen

Abbildung 6: Beispielhafter Entwicklungsprozess für Blockchain-Projekte



abstrakten Beweis wird die Modellierung eines Angreifermodells und von Schutzzielen benötigt. Ein solcher positiver Sicherheitsbeweis benötigt lediglich 20 Seiten. So können hohe nachträgliche Kosten durch konzeptionelle Fehler vermieden werden. Die Möglichkeit von Sicherheitsbeweisen ist in der Informatik bereits seit Jahren bekannt, wird jedoch in der Praxis noch selten umgesetzt. Gemäß einem auf Blockchain-Projekte zugeschnittenen Entwicklungsprozess (siehe Abbildung 6) hat etwa die Firma CryptoTec (zu der zwei Autoren dieses Artikels zählen, Anm. d. Red.) für den selbst entwickelten Blockchain-Dokumentenspeicher entwicklungsbegleitend einen Sicherheitsbeweis geführt, der die Sicherheit, Vertraulichkeit und Integrität von Dokumenten garantiert.

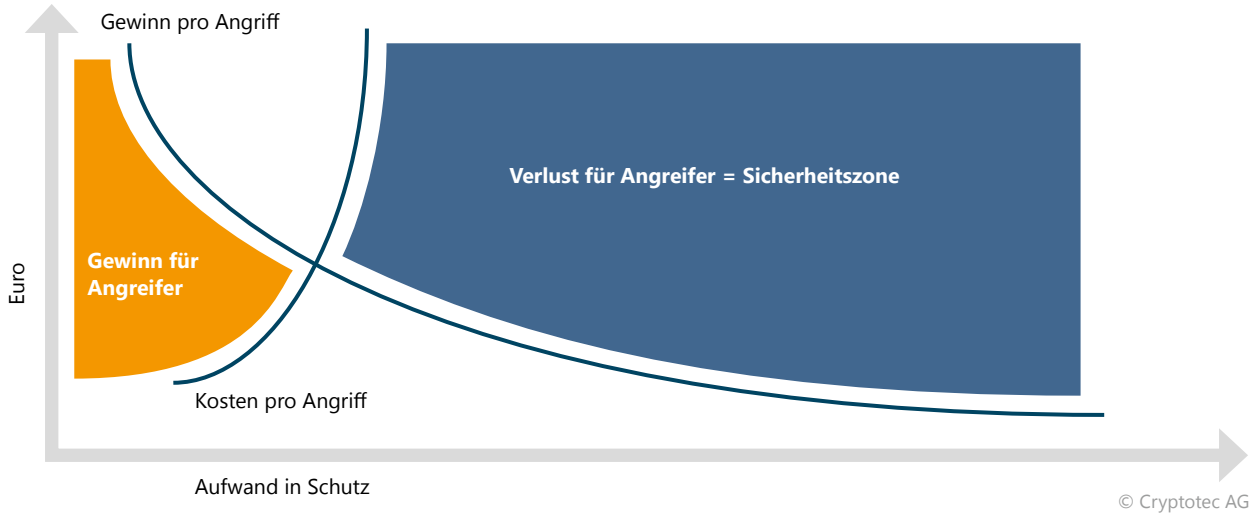
5.2 Angreifermodelle und Schutzziele

> If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?"
>
> Jonathan Katz

Angreifermodelle und Schutzziele modellieren mögliche Szenarien und definieren die Höhe des benötigten Sicherheitslevels. In einem Angreifermodell wird festgelegt, welche Fähigkeiten ein potenzieller Angreifer hat und wie ein Angreifer vorgehen kann. Bei einem Angreifer kann es sich sowohl um eine professionelle Hackergruppe als auch um einen Nutzer handeln, der die Zahlung umgeht.

Entwickler müssen sich in potenzielle Angreifer hineinversetzen, um alle möglichen Angriffsszenarien abzudecken. Wird dabei eine Möglichkeit übersehen, so schränkt es die Sicherheit des ganzen Systems ein. Hierfür braucht es viel Zeit und Erfahrung mit Hackerangriffen. In der Praxis stehen interne Mitarbeiter in Unternehmen häufig unter Zeitdruck und kennen in erster Linie die Perspektive des eigenen Unternehmens, nicht die eines Angreifers. Außerdem gilt folgender Grundsatz in der Informatik: „Ein Entwickler kann sein eigenes System nicht testen." Deshalb ist die Hinzunahme von externen Experten bei der Erstellung eines Angreifermodells beinahe zwingend. Durch einen Wechsel der Perspektive können neue mögliche Angriffsszenarien erarbeitet werden, und die internen Mitarbeiter können sich auf ihr Kerngebiet, die Entwicklung des Systems, konzentrieren.

Abbildung 7: Wirtschaftlichkeit von Angriffen



Schutzziele legen fest, welches Sicherheitslevel ein System benötigt und welche Angriffe verhindert werden sollen. Hierbei gibt es zwei Arten von Schutzzielen:

1. Jeder Angriff soll abgewehrt werden (100-prozentiger Schutz).
2. Angriffe, die wirtschaftlich vorteilhaft für Angreifer sind, sollen abgewehrt werden.

Ein 100-prozentiger Schutz ist ein schwer zu erreichendes Ziel, da zunehmender Schutz eines Systems exponentiell teurer wird. In vielen Fällen reicht es aus, Angriffe für organisierte Kriminalität wirtschaftlich uninteressant zu gestalten. Abbildung 7 zeigt den Gewinn pro Angriff und die Kosten pro Angriff als Funktion. Bei steigendem Schutz des Systems steigen die Kosten für den Angreifer exponentiell an. Sobald die Kosten eines Angriffs größer sind als der Gewinn des Angriffs, wird der Angriff unwirtschaftlich und unattraktiv für organisierte Kriminalität. Es kann also genügen, ein System so sicher zu machen, dass ein Angriff nicht wirtschaftlich ist. Durch die *Blockchain* erhöht sich für einen Angreifer zudem das Risiko, überführt und strafrechtlich verfolgt zu werden. In der Vergangenheit versuchten Hacker, mögliche Spuren auf Servern zu beseitigen, um nicht identifiziert zu werden. In Blockchain-Anwendungen können jedoch Transaktionen nicht nachträglich verändert werden, sondern sind transparent dokumentiert. Das erhöhte Risiko für Angreifer ist ein Vorteil der Blockchain-Technologie und kann letztendlich zur Reduktion der Kosten für Sicherheitsmaßnahmen führen.

5.3 Benutzerfreundlichkeit

> „Complexity is the worst enemy of security."
>
> Bruce Schneier

Der US-amerikanische Experte für Kryptografie und Computersicherheit Bruce Schneier bringt den Zusammenhang von Komplexität und Sicherheit von IT-Systemen auf den Punkt. Ein unnötig kompliziertes Design erschwert nicht nur die Bedienung, sondern sorgt auch für mehr Sicherheitslücken. Eine Anwendung sollte so einfach wie möglich zu bedienen sein und nur die Funktionen enthalten, die tatsächlich benötigt werden. Benutzerfreundliche Software macht, was der Benutzer erwartet. Sichere Software macht das, was der Benutzer erwartet und nichts anderes. Alle weiteren zusätzlichen Funktionen, die der Nutzer nicht braucht, erhöhen die Komplexität eines Systems und beeinträchtigen zugleich die Sicherheit. Diesen Grundsatz sollte man gerade bei

der Entwicklung von Blockchain-Anwendungen vor Augen haben. In einer hochvernetzten Welt sind die Produkte am erfolgreichsten, die leicht zu bedienen und schwer zu hacken sind. Deshalb sollte neben der Sicherheit auch die Benutzerfreundlichkeit bei der Entwicklung von neuen Anwendungen verfolgt werden.

5.4 Entwicklung von Blockchain-Anwendungen

> „Bitcoin is not the kind of software where we can leave so many unresolved bugs that we need a tracker for them."
>
> Satoshi Nakamoto

Es wurde bereits erwähnt, dass Blockchain-Anwendungen eine hohe Qualität aufweisen müssen und keine Fehler enthalten dürfen. Oftmals können Fehler in der Blockchain-Software nicht mehr rückgängig gemacht werden. So sind beispielsweise 500.000 Ethers, umgerechnet etwa 375 Mio. US-Dollar, von Nutzern der Parity *Wallet* eingefroren, da die Entwickler einen folgenreichen Fehler im Code übersehen haben.[13] Bei der Entwicklung von Blockchain-Anwendungen sind Qualitätsmanagement und Auditierung von hoher Wichtigkeit. Es bietet sich daher an, auf bereits entwickelten und auditierten Blockchain-Modulen aufzusetzen. So reduzieren sich die Entwicklungskosten durch Zusammenarbeit mit externen Blockchain-Experten, und die Sicherheit wird durch bereits erprobte Lösungen erhöht.

5.4.1 Definition der Anforderungen

Bei der Entwicklung von neuen Blockchain-Anwendungen ist es zwingend notwendig, die Anforderungen im Vorhinein klar zu definieren. Nur so können die beste Lösung ausgewählt und spätere Probleme verhindert werden. Die Ethereum-Blockchain ist eine sehr beliebte Plattform, um neue Projekte umzusetzen. Das bedeutet jedoch keinesfalls, dass es für jedes Projekt die richtige Plattform ist. Möchte man beispielsweise in einer industriellen Anwendung 1.000 Transaktionen pro Sekunde (TPS) ausführen, dann wird das Ethereum-Netzwerk mit

13 Penke, Gründerszene – Parity-Millionen in Kryptowährung wohl für immer verloren, https://www.gruenderszene.de/fintech/parity-millionen-wallet-protokoll-999, abgerufen am 08.05.2018.

Tabelle 1: Bewertungsmatrix für Blockchain-Anwendungen

Kriterium	Qualifizierungsfrage
Geschwindigkeit	Wie viele Transaktionen können pro Sekunden validiert werden?
Transaktionsgröße	Wie groß können die Daten sein, die pro Transaktion auf der Blockchain gespeichert werden?
Vertraulichkeit	Welche Vertraulichkeit bietet die Blockchain für Informationen auf der Blockchain?
Verfügbarkeit	Wie hoch ist die Verfügbarkeit (in Prozent) der Anwendung?
Prüfbarkeit	Inwieweit kann verifiziert werden, dass die Daten auf der Blockchain korrekt sind?
Erweiterbarkeit	Wie gut kann die Blockchain durch neue Funktionen erweitert werden?
Einstiegshürde	Werden Nutzer auf der Blockchain identifiziert oder können auch anonyme Nutzer partizipieren?
Payment	Können Zahlungen über die Blockchain abgewickelt werden?

aktuell 20 TPS die Anforderungen der Anwendung nicht erfüllen können.[14] Die Bewertung von Anforderungen kann durch eine Bewertungsmatrix für Blockchain-Anwendungen erleichtert werden (siehe Tabelle 1).

5.4.2 Zuständigkeit für Blockchain-Entwicklung

> „Blockchain ist 80% Business und 20% Technik."
>
> William Mougayar

Die unternehmensübergreifende Vereinheitlichung von Prozessen ist ein großer Vorteil der *Blockchain*. Hierbei kommt es oft zur kompletten Umgestaltung von Geschäftsprozessen, auch als *Business Process Reengineering* bezeichnet. Es ist nicht ausreichend, die bestehenden Prozesse auf eine *Blockchain* zu überführen. So entstehen nur Kosten für die Umstellung. Es wird jedoch kein Mehrwert für den Kunden herbeigeführt oder eine Prozessoptimierung erreicht. Nur durch eine komplette Umgestaltung von Geschäftsprozessen werden Wettbewerbsvorteile erzielt und das Kundenerlebnis verbessert. Die *Blockchain* ist daher ein Thema, welches vom Management und der Strategieabteilung eines Unternehmens implementiert werden muss. Einzelnen Fachbereichen hingegen fehlen hierzu der Gesamtüberblick und die Entscheidungskompetenz. Es wäre auch fatal, das Thema *Blockchain* allein an die IT-Abteilung zu delegieren. Der betriebswirtschaftliche Anteil bei Blockchain-Entwicklungen ist deutlich größer als die tatsächliche Programmierung, da *Blockchain* immer Sicherheit und wirtschaftliche Incentivierung beinhaltet. Die Perspektive von Externen kann dabei helfen, ein Unternehmen auch aus einem anderen Blickwinkel zu betrachten.

14 AltcoinToday, Bitcoin and Ethereum vs Visa and Paypal – Transactions per second, https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/, abgerufen am 08.05.2018.

6 Zusammenfassung

Blockchain ist eine Schlüsseltechnologie und kann in Zukunft Einzug in viele Branchen erhalten. Die Technologie hat das Potenzial, bestehende Geschäftsmodelle anzugreifen und durch effizientere Modelle zu ersetzen. Im Vergleich zu herkömmlichen IT-Systemen hat die *Blockchain* mehrere Vorteile. So können beispielsweise Daten, die auf einer *Blockchain* gespeichert werden, nachträglich nicht manipuliert werden. Aufgrund der Trennung von Informations- und Netzwerksicherheit können auch fremde Teilnehmer die *Blockchain* ohne Sicherheitsrisiko nutzen. Die Informationssicherheit wird mittels Kryptografie gewährleistet. Folglich werden keine aufwendigen Schutzmechanismen (VPN oder *Firewall*) benötigt, wie es bei herkömmlichen IT-Systemen der Fall ist. Daten sind nur für diejenigen lesbar, die den geheimen Schlüssel zum Öffnen der Nachricht kennen. Die Geheimhaltung des Schlüssels durch den Eigentümer der Daten ist daher auch essenziell für die Sicherheit der Daten. Die *Blockchain* ist keinesfalls auf die Umsetzung einer digitalen Währung beschränkt. Vielmehr bringt die Technologie Geld-, Informations- und Warenfluss in einem System zusammen. Hierdurch können Prozesse schneller und effizienter ausgeführt werden, was sich letztlich positiv auf das Kundenerlebnis auswirkt. Neben Effizienz und neuen Geschäftsmodellen können Blockchain-Lösungen die Sicherheit von IT-Systemen erhöhen. Bei der Umsetzung von Blockchain-Anwendungen werden in der Praxis jedoch häufig Fehler begangen. Oftmals können solche Fehler nicht durch ein einfaches Update behoben werden, sondern erfordern zusätzlichen Entwicklungsaufwand. Aus diesem Grund sollte bei der Umsetzung von Blockchain-Lösungen die Sicherheit mit Hilfe eines mathematischen Beweises gewährleistet werden. In diesem Zusammenhang müssen alle möglichen Angriffsszenarien modelliert und das erforderliche Sicherheitslevel definiert werden. Internen Mitarbeitern fehlen häufig ausreichende Erfahrung und Kenntnisse, um Blockchain-Lösungen fehlerfrei zu entwickeln. Die Entwicklung von Blockchain-Lösungen sollte durch das Management oder die Strategieabteilung des Unternehmens gesteuert werden, da nicht nur die IT-Abteilung, sondern alle Geschäftsbereiche von Änderungen durch Blockchain-Technologie betroffen sind.

IV

Digital-Ledger-Technologien wie die *Blockchain* fördern die Entstehung neuer, dezentraler Strukturen. Ihre Einordnung in das bestehende Rechtssystem adressiert zahlreiche Unsicherheiten.

Blockchain-Technologie – Gedanken zur Regulierung

Autoren

Oliver Fußwinkel,
Referat Finanztechnologische Innovationen,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

Christoph Kreiterling,
Referat Finanztechnologische Innovationen,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

1 Einleitung

Man nehme Teile der Spieltheorie aus den 1920er Jahren und verbinde sie mit Methoden moderner Verschlüsselung und Netzwerktechnik. So geschah es im Januar 2009 beim Start des Bitcoin-Netzwerks.[1] Seitdem zeigt dieses Netzwerk, dass die dabei verwendete Blockchain-Technologie stabil und zuverlässig funktionieren kann. Was hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) damit zu tun? Es gehört zu ihren gesetzlichen Aufgaben, die Integrität und Stabilität des Finanzsystems zu wahren und das Kollektiv der Verbraucher zu schützen.[2] Bei der Blockchain-Technologie handelt es sich nicht nur um eine rein technologische Entwicklung, es werden hierbei auch aufsichtlich relevante Aspekte berührt – bis hin zu möglichen Implikationen für die Finanzstabilität.[3] Die aufsichtsrechtliche Verortung setzt ein erstes Verständnis der Blockchain–Technologie voraus.

Eine *Blockchain* ist ein öffentliches, unveränderbares, verteiltes digitales Kontobuch, das nur Hinzufügungen erlaubt. „Öffentlich" bedeutet, dass die Daten für jedermann zugänglich sind. Zu privaten *Blockchains* haben nur bestimmte Teilnehmer Zugang. „Unveränderbar" heißt, dass es nahezu unmöglich ist, die einmal gespeicherten und verschlüsselten Daten einer *Blockchain* im Nachhinein zu verändern oder zu löschen. Es ist also nur möglich, neue Daten hinzuzufügen, ähnlich wie etwa bei der kaufmännischen Buchführung, wo Löschungen in

1 Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, abgerufen am 10.07.2018.

2 Vgl. § 4 Finanzdienstleistungsaufsichtsgesetz (FinDAG) und bspw. § 6 des Gesetzes über das Kreditwesengesetz (KWG).

3 Birch/Brown/Parulava, Special issue papers Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis, in: Journal of Payments Strategy & Systems, Vol. 10, No. 2, 2016, pp. 118-131.

der Primanota nicht vorgesehen sind.[4] „Verteilt" bedeutet, dass eine öffentliche *Blockchain* nicht der Kontrolle eines Teilnehmers oder einer Organisation unterliegt. Stattdessen verwaltet und sichert das Netzwerk (also die Gesamtheit aller Teilnehmer) die Daten, und jeder Teilnehmer speichert grundsätzlich eine vollständige Kopie aller Daten. Mit „Kontobuch" ist gemeint, dass sich eine *Blockchain*, wie bei Bitcoin, nicht nur zur Verwaltung und Fortschreibung von Rechnungseinheiten verwenden lässt, sondern dass die gleiche grundlegende Methode auch für nahezu alle anderen Arten von digitalen Aufzeichnungen eingesetzt werden kann.[5]

Die Kernkomponenten einer *Blockchain* bestehen regelmäßig aus einer Verbindung von Kryptografie, Peer-to-Peer-Netzwerktechnik, Konsensmechanismen, Kontobuch und einem Regelwerk, um gültige Transaktionen zu bestimmen.[6] Eine *Blockchain* ist also eine verteilte, nach Stand der Technik fälschungssichere digitale Datenstruktur, die zur Aufbewahrung sämtlicher Arten von werthaltigen Daten eingesetzt werden kann.[7] Eines der wesentlichen Charakteristika von *Blockchains* besteht darin, dass es keine zentrale Instanz gibt, der man vertrauen muss (wie etwa beim *Cloud Computing*), und dass jeder einzelne Teilnehmer in einem Blockchain-Netzwerk, wie etwa bei Bitcoin, von Beginn der Aufzeichnungen an jede einzelne Transaktion selbst prüfen und validieren kann.[8] Die *Blockchain* setzt also kein Vertrauen in einen Intermediär voraus, da sie den Beteiligten selbst die Schaffung des Vertrauens ermöglicht.

4 Vgl. §§ 238ff. Handelsgesetzbuch (HGB) in Verbindung mit der Anwendung des BMF-Schreibens vom 14.11.2014, GZ IV A 4 - S 0316/13/10003, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

5 MIT Technology Review, Explainer: What is a blockchain? Where it came from, what it does, and how you make one, https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/, abgerufen am 10.07.2018.

6 Hileman/Rauchs: 2017 Global Blockchain Benchmarking Study.

7 Kreiterling/Mögelin, Blockchain – ein Thema für die Finanzaufsicht?, in: Zeitschrift für das gesamte Kreditwesen, Nr. 11/2017, Seite 528.

8 Greenspan, Payment and exchange transactions in shared ledgers, in: Journal of Payments Strategy & Systems, Vol. 10, No. 2, 2016, pp. 172-180.

2 Entstehung dezentraler Ökosysteme und der Blockchain-Ökonomie

Eine der Kernfragen nachhaltigen Wirtschaftens lautet, wie Vertrauen zwischen Unbekannten etabliert wird, um Transaktionen zu ermöglichen.[9] Dies ermöglichen bisher Intermediäre wie Banken und Zentralverwahrer, deren Rolle allerdings dazu führt, dass die Transaktionskosten steigen und die Märkte weniger effizient sind.[10] Die Blockchain-Technologie kann dazu beitragen, das erforderliche Vertrauen und somit die Transaktionskosten zwischen den Transaktionsbeteiligten zu minimieren, etwa indem die Abhängigkeit von Intermediären verringert wird. Zum Hintergrund: Probleme, die sich aus dem Missbrauch von Vertrauen ergeben, wie etwa Betrug, haben erhebliche negative Auswirkungen auf Wirtschaft und Handel; so werden die weltweiten Schäden durch Betrug auf mehr als vier Billionen US Dollar geschätzt.[11] Durch den Einsatz der Blockchain-Technologie soll das notwendige Vertrauen zwischen den Transaktionsbeteiligten verringert werden, indem die Teilnehmer Aktionen innerhalb des Netzwerks selbst und unabhängig prüfen können (Selbstüberprüfbarkeit).[12] Die hierdurch geschaffene Öffentlichkeit soll auf Fehlverhalten abschreckend wirken und eine jederzeitige anlasslose Prüfung ermöglichen. Durch die Blockchain-Technologie könnte daher eine neue Art von dezentralem Ökosystem entstehen: eine Blockchain-Ökonomie. In solchen dezentralen Ökosystemen würden vereinbarte Transaktionen autonom nach Regeln, die etwa durch *Smart Contracts* definiert sind, ausgeführt und weitgehend durchgesetzt.[13]

Dezentrale Ökosysteme würden sich darüber hinaus in einer neuen Form der Organisationsgestaltung manifestieren, die sich etwa an in der *Blockchain* festgelegten Regeln orientiert.[14]

Die Entstehung dezentraler Ökosysteme wirkt sich auf die klassisch-etablierten Wertschöpfungsketten der Finanzdienstleistungsindustrie aus. Waren diese in der Vergangenheit auf Informationstransfer ausgerichtet, deren primärer geschäftlicher Vorteil in der Nutzung von Informationsasymmetrie lag,[15] hat sich die Situation schon durch das Aufkommen von Fintechs[16] geändert.[17] Diese innovativen, mit technischen Lösungen auf einzelne Teile der Wertschöpfungskette spezialisierten Unternehmen sorgen unter anderem dafür, dass die einheitlichen Wertschöpfungsketten der Finanzdienstleistungsindustrie stärker fragmentiert werden.[18]

In dezentralen Ökosystemen in Form von Blockchain-Ökonomien sind die einzelnen Glieder der Wertschöpfungsketten in potenziell viel höherem Maße betroffen. Auch der Wettbewerb um die Besetzung der Kundenschnittstelle[19], die unter anderem zur Bildung von Plattformökonomien führt, würde durch die Blockchain-Ökonomie beeinflusst. Hier müsste man nicht einem Plattform-Betreiber vertrauen, der als Intermediär langfristig höhere Transaktionskosten verursachen kann.

9 Pearce/Warford, World without end: economics, environment, and sustainable development, 1. Aufl. 1993.

10 Coase, The nature of the firm, in: Economia, Vol. 4, No. 16, 1937, pp. 386-405.

11 Gee/Button, The Financial Cost of Fraud 2017: the latest data from around the world, https://brand.crowe.co.uk/wp-content/uploads/sites/2/2017/02/crowe-the-financial-cost-of-fraud-2017.pdf, abgerufen am 10.07.2018.

12 Peters/Panayi, Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, in: Tasca/Aste/Pelizzon/Perony, Banking Beyond Banks and Money. New Economic Windows, 2016, pp. 239-278.

13 Szabo, The idea of smart contracts, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html, abgerufen am 10.07.2018. Als letzte Durchsetzungsinstanz formellen Rechts fungierten in einem demokratischen Rechtsstaat weiterhin die Gerichte, aber die zwischen den Parteien vertraglich vereinbarten Regeln kämen in einer Blockchain-Ökonomie tatsächlich weitgehend zur automatisierten dezentralen Durchsetzung.

14 Beck/Müller-Bloch/King, Governance in the Blockchain Economy: A Framework and Research Agenda, https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda, abgerufen am 10.07.2018.

15 Healy/Krishna/Palepu, Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature, in: Journal of accounting and economics 31.1-3, 2001, pp. 405-440.

16 Eine allgemeingültige Definition des Begriffs Fintechs existiert bisher nicht. Als Kombination aus den Worten *Financial Services* und *Technology* versteht man unter Fintechs gemeinhin junge Unternehmen, die mit Hilfe technologiebasierter Systeme spezialisierte und besonders kundenorientierte Finanzdienstleistungen anbieten.

17 Alt/Ehrenberg, Fintech - Umbruch der Finanzbranche durch IT in: Wirtschaftsinformatik & Management 03/2016, Seite 8-17.

18 Chiu, Fintech and Disruptive Business Models in Financial Products, Intermediation and Markets-Policy Implications for Financial Regulators, in: Journal of Technology Law and Policy, Vol. 21 (1), 2016, pp. 55-112.

19 Goodwin, The battle is for the customer interface, https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/, abgerufen am 10.07.2018.

Die Blockchain-Ökonomie hat ihre eigene Infrastruktur-Plattform, die von ihren Teilnehmern geschaffen und kontrolliert wird.[20] Somit besetzt das Blockchain-Netzwerk nicht nur die Kundenschnittstelle unmittelbar und kontrolliert sie dezentral. Sie bindet sehr viel stärker als bisherige Lösungen Beteiligte in den Transaktionsprozess ein. In diesen dezentralen Ökosystemen können durch die Blockchain-Technologie und die eingesetzten Verfahren nicht nur Informationen übertragen werden, sondern auch Werte.[21]

Eine solch umfangreiche Änderung der Technologieinfrastruktur der Finanzdienstleistungsindustrie beträfe nicht nur die eingesetzten Systeme (welche Technik wird eingesetzt?) und hörte auch nicht bei den Geschäftsprozessen auf (Organisation, *Governance*, wie und mit wem sollen Ziele erreicht werden?). Das skizzierte Potenzial der Blockchain-Technologie könnte auch erhebliche Auswirkungen auf die Strategie (was wird gemacht?) der Unternehmen in der Finanzdienstleistungsindustrie haben. Somit hätte die Blockchain-Technologie potenzielle Auswirkungen auf die Ebenen Strategie, Prozesse und Systeme.[22] Wer die Blockchain-Technologie nur unter dem Aspekt der Kostenreduzierung betrachtet, der könnte die Ertragspotenziale übersehen.

Fragen von Strategie, Prozessen und Systemen im Zusammenhang mit der Blockchain-Ökonomie sind wichtig, allerdings sind auch erfolgskritische Details entscheidend: So ist etwa noch fraglich, wie bestehende Anforderungen, etwa der europäischen Datenschutz-Grundverordnung (DSGVO)[23] und das darin enthaltene „Recht auf Vergessenwerden"[24] mit den derzeit bekannten Verfahren auch durch die Blockchain-Technologie vollumfänglich umgesetzt werden könnten.

Zudem kennt das Sicherheits- und Schutzniveau von derzeitigen Blockchain-Lösungen nur eine Stufe: So existieren nach dem *Defence in Depth Approach* des ISO-Sicherheits-Standards 27033[25] mehrere Stufen für ein maximal mögliches Sicherheits- und Schutzniveau der Daten. Demnach bietet etwa die Schutzstufe „Perimeter" das höchste Sicherheits- und Schutzniveau. Das niedrigste Niveau bietet hingegen der Schutz auf „Data"-Level. Alle Daten, die in derzeitigen *Blockchains* abgelegt werden (Daten *On-Chain*), befinden sich auf dem „Data"-Level. Es ist daher fraglich, inwiefern eine Blockchain-Lösung die von den beaufsichtigten Unternehmen definierten Schutzbedarfe im Rahmen des Informationsrisikomanagements sicherstellen kann.

20 Underwood, Blockchain beyond bitcoin, in: Communications of the ACM, Vol 59, No. 1, 2016, pp. 15-17.

21 Church, MIT Management School, Blockchain, explained, An MIT expert on why distributed ledgers and cryptocurrencies have the potential to affect every industry, http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/, abgerufen am 10.07.2018.

22 Österle/Blessing, Business Engineering Modell in: Österle/Winter, Business Engineering: Auf dem Weg zum Unternehmen des Informationszeitalters, 2. Aufl. 2003, Seite 65-85.

23 Verordnung (EU) Nr. 2016/679, ABl. L 119/1.

24 Art. 17 DSGVO.

25 ISO/IEC 27033-2:2012(en) Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security, http://www.iso.org/standard/51581.html, abgerufen am 04.07.2018.

3 Grundsätzliche Herangehensweise der BaFin

Die Blockchain-Technologie hat branchenübergreifend große Innovationskraft und das Potenzial, gerade die Finanzindustrie in vielerlei Hinsicht zu beeinflussen, etwa den Zahlungsverkehr und den Wertpapierhandel, die Vermögensverwaltung und das Kreditwesen. Art und Ausmaß dieser Auswirkungen lassen sich noch nicht abschließend bestimmen. Hervorzuheben ist aber der bereits erwähnte Bedeutungsverlust von Intermediären in einer Blockchain-Ökonomie. Bislang beaufsichtigt die BaFin hauptsächlich Unternehmen mit Intermediärsfunktion, wie Kreditinstitute. Doch auch in einer künftigen Blockchain-Ökonomie müssen die übergeordneten Ziele der Integrität und Stabilität des Finanzsystems sowie des kollektiven Verbraucherschutzes erfüllbar bleiben. Kinderkrankheiten der Technologie sollten zur Vorsicht mahnen und die derzeit verbreitete unkritische Innovationsbegeisterung eindämmen, den Blick auf die Potenziale aber nicht verstellen.

Bei der Befassung mit Kryptotoken und generell mit innovativen Finanztechnologien lässt sich die BaFin stets vom Grundsatz der Technologieneutralität leiten und folgt dem Credo „gleiches Geschäft, gleiches Risiko, gleiche Regulierung“. Sie wahrt damit auch weiterhin die rechtsstaatlichen Prinzipien von Verhältnismäßigkeit und Gleichbehandlung.

4 ICOs und Kryptotoken: Risiken und aufsichtsrechtliche Einordnung

Erscheinungsformen der Blockchain-Ökonomie sind bereits heute am Finanzmarkt feststellbar und lassen aufsichtsrechtliche Implikationen erkennen. Neben der digitalen Abbildung bislang papierbasierter Prozesse und Produkte wie der blockchainbasierten Platzierung einer Anleihe[26] und der Außenhandelsfinanzierung über Akkreditive[27] sind auch neue Konstruktionen mit disruptivem Charakter zu beobachten. Hierzu gehören etwa die seit 2017 stark zunehmenden Kapitaleinsammlungen über *Initial Coin Offerings* (ICO)[28], die aufgrund ihrer aktuellen Bedeutung für Anleger, Investoren und Emittenten hier näher betrachtet werden sollen. Von grundsätzlicher Bedeutung, nicht nur im Kontext von ICOs, ist auch die aufsichtsrechtliche Einordnung der vielfältigen Möglichkeiten der digitalen Wertabbildung in einer *Blockchain* über Kryptotoken[29]. Im Folgenden wird daher zunächst eine allgemeine aufsichtsrechtliche Verortung verschiedener Untergruppen von Kryptotoken vorgenommen und sodann auf Besonderheiten und Risiken ihrer Emission mittels eines ICOs eingegangen.

4.1 Kryptotoken

Jeder Kryptotoken kann andere Funktionen und Eigenschaften haben. Einige *Token* sind fester Bestandteil einer bestimmten *Blockchain*, wie etwa Bitcoin für die Bitcoin-Blockchain und Ether für Ethereum. Daneben können durch *Smart Contracts* wie etwa bei Ethereum diverse funktionsbezogene *Token* geschaffen werden. Diese *Token* werden dann auf einer bestehenden Blockchain-Infrastruktur (in diesem Fall Ethereum) geschaffen und verwaltet. Da *Smart Contracts* prinzipiell frei programmierbar sind und die entsprechenden *Token* daher höchst unterschiedlich ausfallen, lässt sich der einzelne *Token* verlässlich nur auf Grundlage einer Einzelfallbetrachtung aufsichtsrechtlich einordnen.

Die hierauf gerichtete Kritik, die verständlicherweise nach einfachen Lösungen ruft, verkennt die vielfältigen Gestaltungsmöglichkeiten und die große Bandbreite der technischen Eigenschaften von *Token*. Sie verkennt, dass Programmierer und Vertrieb in der Begriffsbildung frei sind; für vergleichbare und im Wesentlichen sogar identische *Token* mag es tausend verschiedene Begriffe geben, unterdessen können unter ein- und demselben Begriff eine Vielzahl unterschiedlicher *Token* gehandelt werden. Die Kritik verkennt auch, dass die pauschale Einordnung unterschiedlicher *Token* in bestimmte aufsichtsrechtliche Kategorien in einer Vielzahl von Fällen zu in der Sache nicht gerechtfertigten Ergebnissen führen wird und eventuell den Raum für Innovationen einschränkt. Sie verkennt ebenso, dass regulatorische Vorgaben in Gestalt von unspezifischen Allgemeindefinitionen faktisch zu Standardisierungen führen, die den Raum für Innovationen zumindest einschränken. Auch dürften solche Vorgaben kaum den rechtlichen Grundvoraussetzungen an regulatorisches wie aufsichtliches Handeln Rechnung tragen, namentlich dem Grundsatz der Gesetzesbindung der Verwaltung, dem Übermaßverbot und dem Gleichbehandlungsgebot.[30]

Grundsätzlich kann man Kryptotoken verstehen als eine digitale Abbildung eines intrinsischen oder marktseitig zugesprochenen Wertes durch Nutzung der *Distributed Ledger Technology* (DLT)[31]. Diese auf einen Wert abstellende Definition betont insbesondere die vorherrschende

26 Daimler Pressemeldung, Daimler und LBBW setzen erfolgreich Blockchain bei Schuldschein-Transaktion ein, http://media.daimler.com/marsMediaSite/de/instance/ko/Daimler-und-LBBW-setzen-erfolgreich-Blockchain-bei-Schuldschein-Transaktion-ein.xhtml?oid=22744703, abgerufen am 03.07.2018.

27 Zim Pressemeldung, ZIM's Groundbreaking Blockchain-Based Bill of Lading, http://www.zim.com/news/press-releases/zims-groundbreaking-blockchain-based-bill-of-lading, abgerufen am 03.07.2018.

28 Oft auch und zutreffender als "Token Generating Events" oder "Token Sales" bezeichnet.

29 Um einen Begriff zu verwenden, der zugleich wertfrei und präzise ist, wird für diesen Artikel der Begriff „Kryptotoken" verwendet. Die Bezeichnung ist neutral und impliziert im Gegensatz zu den anderen Begriffen wie etwa „Kryptowährungen", „Crypto Assets" und „virtuelle Währungen" keine Charakteristika, die Kryptotoken nicht notwendigerweise innewohnen.

30 Zum Übermaßverbot, vgl. Grzesick, in: Maunz/Dürig, Grundgesetz-Kommentar, 82. EL 2018, Art. 20 Rn. 107.

31 Die Distributed-Ledger-Technologie definiert die Bank for International Settlements (BIS) wie folgt: „DLT refers to the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes", BIS, Distributed ledger technology in payment, clearing and settlement, http://www.bis.org/cpmi/publ/d157.htm, abgerufen am 03.07.2018.

Nutzung von Kryptotoken als Investitionsgegenstand, ohne eine Vorfestlegung zu treffen, ob der jeweilige *Token* eine Forderung oder Verpflichtung einer Entität umfasst oder in seiner Funktionalität sonstige Zahlungsströme zugunsten des Inhabers auslöst.

Von Bedeutung sein wird auch der Begriff der „virtuellen Währung" in Art. 1 (2) (d) der 5. Geldwäscherichtlinie, der alle potenziellen Verwendungszwecke von virtuellen Währungen abdecken soll: „Digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann".[32]

Kryptotoken sind nicht per se unreguliert, sondern unterfallen – je nach konkreter Ausgestaltung im Einzelfall – der bestehenden Finanzmarktregulierung. Sie werden also nicht pauschal, sondern spezifisch und technologieneutral nach materiellen Tatbeständen (und nicht Marketingerwägungen) reguliert, die der juristischen Auslegung unterliegen und damit auch neuartige Sachverhalte erfassen können.

Der konkrete Einzelfall entscheidet also über die aufsichtsrechtliche Beurteilung eines kryptotokenbasierten Geschäftsmodells. Nach den bisherigen Erfahrungen bei der Überprüfung von Geschäftsmodellen im Zusammenhang mit Kryptotoken erweisen sich vor allem Regelungen aus dem Kreditwesengesetz (KWG), dem Wertpapierhandels- und dem Wertpapierprospektgesetz (WpHG, WpPG) und dem Vermögensanlangengesetz (VermAnlG) als prüfungsrelevant. Daneben kommen zahlreiche weitere Elemente der Finanzmarktregulierung in Betracht, wie insbesondere das Geldwäschegesetz (GwG), das Zahlungsdiensteaufsichtsgesetz (ZAG), das Kapitalanlagegesetzbuch (KAGB), aber auch unmittelbar anwendbares europäisches Sekundärrecht wie die EU-Marktmissbrauchsverordnung (Market Abuse Regulation – MAR)[33].

Klarheit über die aufsichtsrechtliche Einordnung eines konkreten Vorhabens im Zusammenhang mit Kryptotoken kann – nach Lektüre der Informationen auf

32 RL (EU) 2018/843, ABl. L 156/43.

33 Verordnung (EU) Nr. 596/2014, ABl. L 173/1.

www.bafin.de – im Wege der Einholung einer Auskunft von der BaFin gewonnen werden, die als eine Form des schlicht-hoheitlichen Handelns grundsätzlich keinen Regelungscharakter hat (§ 24 Verwaltungsverfahrensgesetz – VwVfG).

Darüber hinaus sehen die Aufsichtsgesetze in Zweifelsfällen eine – gebührenpflichtige[34] – Feststellungsbefugnis der BaFin für die Frage vor, ob ein Unternehmen der Aufsicht nach dem KWG, VAG, KAGB oder ZAG unterliegt.[35] In der Praxis kommt eine solche Regelung im Wege der Einzelfeststellung nur in besonders gelagerten Fällen in Betracht, da die Behörde nach allen vier einschlägigen Gesetzen bei Feststellung eines unerlaubten Geschäftsbetriebs grundsätzlich im Wege einer Einstellungs- und/oder Abwicklungsanordnung einschreiten kann und im Regelfall auch muss (intendiertes Ermessen). Im umgekehrten Fall ergibt ein Negativtestat im Hinblick auf die eventuelle Erlaubnispflicht eines Geschäftsvorhabens nur als Auskunft, grundsätzlich ohne Regelungscharakter, Sinn, da die Behörde nicht feststellen kann, dass das Unternehmen nicht dem Erlaubnisvorbehalt unterliege, solange sie nicht das gesamte Geschäft dieses Unternehmens geprüft hat. In beiden Fällen bietet das Kontaktformular für Unternehmensgründer der BaFin eine Möglichkeit zum unkomplizierten, kostenlosen und digitalen Erstkontakt.[36]

34 §§ 14 FinDAG i.V.m. § 2 Abs. 1 und Anlage 1 Nr. 1.1.8.1. FinDAGKostVO; die Gebührenhöhe beträgt 10.000,00 €.

35 vgl. § 4 KWG, § 4 VAG, § 5 Abs. 3 KAGB und § 4 Abs. 4 ZAG.

36 https://www.bafin.de/SiteGlobals/Forms/Kontakt/Fintech_Integrator.html.

Jenseits der rechtlich relevanten gesetzlichen Tatbestandsmerkmale und ihrer Auslegung durch die BaFin beziehungsweise die höchstrichterliche verwaltungsgerichtliche Rechtsprechung lassen sich Kryptotoken zwecks einfacher Darstellung[37] in drei Kategorien einteilen:

- *Payment-Token* (wie Bitcoin): Ihnen kommt meist exklusiv oder unter anderem die Funktion eines privaten Zahlungsmittels zu, und sie verfügen regelmäßig über keinen intrinsischen Wert. Darüber hinaus besteht keine oder nur geringe weitere Funktionalität.
- Wertpapierähnliche *Token* (*Equity*- und sonstige *Investment-Token*): Nutzer haben mitgliedschaftliche Rechte oder schuldrechtliche Ansprüche vermögenswerten Inhalts, ähnlich wie bei Aktien und Schuldtiteln.
- *Utility-Token* (*App-Token*, Nutzungstoken, Verbrauchstoken): Sie können nur im Netzwerk des Emittenten zum Bezug von Waren oder Dienstleistungen genutzt werden. Bei *Utility-Token* finden sich regelmäßig sehr komplexe rechtliche Gestaltungen.

4.1.1 Payment-Token und sogenannte virtuelle Währungen

Bei Payment-Token wie Bitcoin, Ether und Ripple handelt es sich nicht um Währungen im engeren Sinne, die der Verfassungsordnung des Geldwesens eines Staates entsprechen.[38] Rechtlich betrachtet wären demnach nur gesetzliche Zahlungsmittel und die an gesetzliche Zahlungsmittel anknüpfenden Giralguthaben bei staatlich zugelassenen Kreditinstituten, letztere despektierlich auch als Fiatgeld bezeichnet, als Währungen zu qualifizieren. Ökonomisch betrachtet dient eine Währung allerdings als Zahlungsmittel, als Wertaufbewahrungsmittel und als Rechnungseinheit. Diese Eigenschaften hängen unmittelbar miteinander zusammen. Keine dieser ökonomischen Eigenschaften wird regelmäßig in ausreichendem Maße von Kryptotoken wie Bitcoin erfüllt. Auch ähneln Kryptotoken weder in ihrem Wertverlauf noch in ihren Merkmalen Währungen oder klassischen Vermögensanlagen. Sie stellen somit ökonomisch keine Währung dar, sondern sind eher als Spekulationsobjekt zu betrachten.[39]

Die BaFin hat Bitcoins und vergleichbare sogenannte virtuelle Währungen bereits mit Aufnahme in das Merkblatt „Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG)“ vom 22. Dezember 2011 aufsichtlich bewertet. Das Merkblatt ist mittlerweile im Zuge der Umsetzung der zweiten Zahlungsdienste-Richtlinie novelliert worden. Doch schon seinerzeit führte es – inhaltlich immer noch zutreffend – aus:

„Der E-Geld-Begriff ist ein […] rechtstechnischer Begriff, der typologisch lediglich bestimmte Teile des wirtschaftlichen Phänomens des elektronischen Geldes abbildet. Unabhängig davon, ob computernetz-, server- oder kartengebundene elektronische Werteinheiten in der wirtschaftlichen Realität als Zahlungsmittel fungieren, liegt E-Geld insbesondere nur dann vor, wenn dieses gegen Zahlung eines Geldbetrages ausgestellt wird. […] Als Zahlungsmittel bestimmte Werteinheiten, die in Barter-Clubs, privaten Tauschringen oder anderen Zahlungssystemen gegen realwirtschaftliche Leistungen, Warenlieferungen oder Dienstleistungen geschöpft oder wie z.B. die Bitcoins gegenleistungslos in Computernetzwerken erschaffen werden, scheiden damit aus dem Tatbestand des E-Geldes aus, auch wenn sie wirtschaftlich die gleiche Funktion wie E-Geld haben und unter Geldschöpfungsgesichtspunkten das eigentliche Potential privat generierter Zahlungsmittel stellen (siehe hierzu auch die RegBegr. zu § 1a Abs. 3, BT-Drucks. 17/3023, Seite 40). […] mit der Streichung des Tatbestandes des Netzgeldgeschäftes (§ 1 Abs. 1 Satz 2 Nr. 12 KWG) in der Fassung der 6. KWG-Novelle wurde der Aspekt privater Geldschöpfung ausgeblendet.“

Damit hat die BaFin nicht nur die regelmäßige Nichtanwendbarkeit des E-Geld-Tatbestandes in § 1 Abs. 2

37 Hybride Formen von *Token* sind möglich und kommen nicht selten vor.

38 Vgl. § 14 Abs. 1 Satz 2 Gesetz über die Deutsche Bundesbank, Verordnung (EG) Nr. 974/98, Artikel 10 vom 01.01.2002.

39 Thiele/Diehl, Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?, in: ifo Schnelldienst 70, Nr. 22, 2017, Seite 3-20.

Satz 3 ZAG auf den Großteil der damals bekannten virtuellen Währungen begründet.[40] Sie hat zugleich belegt, dass es sich bei der Streichung des Netzgeldtatbestandes durch das Vierte Finanzmarktförderungsgesetz[41] zum 1. Juli 2002 um eine bewusste Entscheidung des Gesetzgebers handelte, den früheren Tatbestand des Netzgeldes, das die 6. KWG-Novelle (Inkrafttreten 1. Januar 1998) noch als Bankgeschäft unter § 1 Abs. 1 KWG geregelt hatte, im Zuge der Umsetzung der Ersten E-Geld-Richtlinie abzuschaffen. Dieser Netzgeldgeschäftstatbestand erfasste die „Schaffung und die Verwaltung von Zahlungseinheiten in Rechnernetzen", was nicht nur das spätere E-Geld im Sinne der EU-E-Geld-Richtlinien abgedeckt, sondern über diesen Tatbestand auch jede andere Art von virtuellen Rechnungseinheiten eingeschlossen hätte, die, wie Bitcoin, gegenleistungslos geschaffen als eine Art privates Nebengeld neben die gesetzlichen Zahlungsmittel hätten treten sollen.

Geradezu visionär im Hinblick auf spätere Entwicklungen liest sich die seinerzeitige Begründung des Gesetzgebers für die Schaffung des Netzgeldtatbestandes im Jahr 1997: „Das Netzgeld wird dabei vom Benutzer auf PC-Festplatte gespeichert und einmalig oder auch mehrfach zur Abwicklung von Fernzahlungen durch Dialog zwischen den beteiligten Rechnern verwendet, wobei moderne kryptographische Verfahren vor Fälschungen oder Verfälschungen Schutz bieten sollen. Die Zahlungen werden in der Regel wie mit Bargeld anonym durchgeführt."[42]

Mit der Streichung dieses Tatbestandes, der sich liest, als sei er auf die erst Jahre später entstehenden virtuellen Währungen auf Blockchain-Basis zugeschnitten worden, wurde klargestellt, dass die Schaffung und erst recht die bloße Nutzung von virtuellen Währungen als Ersatz für Bargeld oder Buchgeld für sich genommen keine erlaubnispflichtigen Tätigkeiten darstellen. Virtuelle Währungen können also zum Ausgleich von Zahlungsverpflichtungen zwischen den beteiligten Nutzern verwendet werden. Ebenso stellt das *Mining* solcher *Token* grundsätzlich keine erlaubnispflichtige Tätigkeit dar, da der *Miner* die *Token* zumindest in einem dem Bitcoin vergleichbaren System nicht selbst emittiert oder platziert.

Eine andere Regelung aus der 6. KWG-Novelle ist jedoch bewusst erhalten geblieben, nämlich die Einstufung von Rechnungseinheiten als Finanzinstrumente (nur) im Sinne des KWG nach § 1 Abs. 11 Satz 2 Nr. 7 KWG. Damit wurde die Möglichkeit belassen, über die Erlaubnispflichten für Geschäfte mit Finanzinstrumenten Schutzlücken in Bezug auf virtuelle Währungen gerade auch in der Geldwäscheprävention nach wie vor zu adressieren, ohne in einen Konflikt zwischen dem früheren Netzgeldgeschäft als Bankgeschäft und der harmonisierten Regulierung des E-Geld-Geschäftes zu geraten.

2011 hat die BaFin Bitcoins und vergleichbare Zahlungstoken als Finanzinstrumente in der Form von Rechnungseinheiten gemäß § 1 Abs. 11 Satz 1 KWG qualifiziert. Dies sind Einheiten, die mit Devisen vergleichbar sind und nicht auf gesetzliche Zahlungsmittel lauten. Hierunter fallen Werteinheiten, die die Funktion von privaten Zahlungsmitteln bei Ringtauschgeschäften haben, sowie jede andere Ersatzwährung, die aufgrund privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt wird. Auf einen zentralen Emittenten kommt es hierbei nicht an.[43] Die oben ausgeführte währungsrechtliche Zulässigkeit ist für die Beurteilung als Rechnungseinheit und somit als Finanzinstrument im Sinne des KWG dagegen unerheblich.[44]

Treten neben der Nutzung als Zahlungsmittel oder dem *Mining* von Zahlungstoken also weitere Umstände hinzu, kann eine Erlaubnispflicht ausgelöst werden – besonders dann, wenn ein Markt geschaffen wird, auf dem diese gehandelt werden können. Der gewerbsmäßige

40 Damals § 1a Abs. 3 ZAG a.F. Entscheidend ist aber immer die Prüfung im Einzelfall.

41 Viertes Finanzmarktförderungsgesetz, BGBl. I 2002, Seite 2010.

42 Regierungsentwurf zur Umsetzung von EG-Richtlinien zur Harmonisierung bank- und wertpapieraufsichtsrechtlicher Vorschriften vom 6.4.1997 (6. KWG-Novelle), BT-Drs. 13/7142, Seite 64.

43 Vgl. BaFinJournal Januar 2014, Seite 26 ff.

44 BaFin Merkblatt, Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 3 KWG (Aktien, Vermögensanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstrumente, Devisen, Rechnungseinheiten und Emissionszertifikate), www.bafin.de/dok/7852552, abgerufen am 10.07.2018.

Rücktausch von Bitcoin in Euro steht grundsätzlich unter Erlaubnisvorbehalt nach § 32 Abs. 1 KWG. Die Dienstleistung ist als Finanzkommissionsgeschäft (§ 1 Abs. 1 Satz 2 Nr. 4 KWG) zu qualifizieren, wenn der Dienstleister die Bitcoins in Kommission nimmt, um sie für Rechnung des Kunden am Markt an einen Dritten zu veräußern. Im Fall einer offenen Stellvertretung, die praktisch nicht relevant werden dürfte, wäre die Dienstleistung als Abschlussvermittlung nach § 1 Abs. 1a Satz 2 Nr. 2 KWG einzustufen. Wird die Transaktion über einen Kaufvertrag zwischen Dienstleister und Kunden geregelt, ist das Geschäft als Eigenhandel nach § 1 Abs. 1a Satz 2 Nr. 4 KWG einzuordnen. Hierzu zählen regelmäßig Anbieter, die als Exchange-Trader, virtuelle Wechselstuben oder mit BTC-Automaten einen direkten Umtausch gängiger Währungen in *Payment-Token* anbieten.

Sofern der Rücktausch der Zahlungstoken nicht unmittelbar zwischen den am Rücktausch beteiligten Vertragsparteien, sondern unter Einschaltung eines Dritten (etwa einer Internet-Plattform, die als Instanz für den Tausch des virtuellen Geldes in gesetzliche Zahlungsmittel fungiert) erfolgt, kommt außerdem eine Erlaubnispflicht nach § 10 Abs. 1 ZAG wegen Erbringens von Zahlungsdiensten in Betracht. Leitet der Dritte den realen Gegenwert der virtuellen Währung im Auftrag des Erwerbers über sein Konto an den Tauschempfänger weiter, betreibt der Dritte das Finanztransfergeschäft (§ 1 Abs. 1 Satz 2 Nr. 6, 1. Alt. ZAG). Wird er im Auftrag des Zahlungsempfängers tätig, erfüllt er unter Umständen den Tatbestand des Akquisitionsgeschäfts i.S.d. § 1 Abs. 1 Satz 2 Nr. 5, 2. Alt. ZAG. Auch eine Kombination beider Tatbestände ist denkbar, wenn der Zahlungsdienstleister für beide Seiten des Tauschgeschäfts tätig wird (was bei Internet-Plattformen oft der Fall ist). Entscheidend sind – wie immer bei einer Beurteilung der Erlaubnispflicht – die konkreten vertraglichen Absprachen zwischen den Beteiligten.
Die genaue Abgrenzung kann im Einzelfall schwierig sein, insbesondere wenn die Geschäftsbedingungen nicht nach rechtlichen Standards ausgestaltet sind.[45]

45 Vgl. BaFinJournal Januar 2014, Seite 26 ff., und www.bafin.de/dok/7906360.

Erlaubnispflichten nach Kreditwesengesetz führen dann zur Verpflichteteneigenschaft nach § 2 Geldwäschegesetz (GwG), und die Verpflichteten müssen insbesondere allgemeine Sorgfaltspflichten (§ 10 GwG) und Aufzeichnungs- und Aufbewahrungspflichten (§ 8 GwG) erfüllen sowie interne Sicherungsmaßnahmen treffen (§ 6 GwG) und in Verdachtsfällen Meldungen an die Financial Intelligence Unit (FIU) erstatten (§ 43 GwG).

4.1.2 Wertpapierähnliche Token

Eine Vielzahl von Kryptotoken der neueren Generation, insbesondere jene, die im Rahmen von *Initial Coin Offerings* (ICOs)/*Token Generating Events* (TGEs) emittiert werden, bilden einen intrinsischen Wert für den Inhaber des dazugehörigen privaten Schlüssels ab (*Equity*- und *Investment-Token*). Das kann nicht weiter verwundern, da die Möglichkeit der digitalen Übertragung von Werten ohne Intermediäre einen der Kernaspekte einer Blockchain-Ökonomie ausmacht.

Abhängig von der Rechtsposition, die diese *Token* vermitteln, kann es sich dabei um Wertpapiere im Sinne des § 2 Abs. 1 WpHG handeln. Entgegen dem Wortlaut stellt schon die gesetzliche Definition klar, dass es auf Papier nicht ankommt. Ausreichend ist, dass Transaktionen anhand der Distributed Ledger- oder Blockchain-Technologie so dokumentiert werden können, dass die in den *Token* verkörperten Rechte eindeutig einer Adresse (nicht zwingend einem Namen) zugeordnet werden können:

„Wertpapiere im Sinne des Wertpapierhandelsgesetzes sind, auch wenn keine Urkunden über sie ausgestellt sind, alle Gattungen von übertragbaren Wertpapieren mit Ausnahme von Zahlungsinstrumenten, die ihrer Art nach auf den Finanzmärkten handelbar sind, insbesondere Aktien, andere Anteile an in- oder ausländischen juristischen Personen, Personengesellschaften und sonstigen Unternehmen, soweit sie Aktien vergleichbar sind, sowie Hinterlegungsscheine, die Aktien vertreten, Schuldtitel, […]“.

Diese Definition setzt den Wertpapierbegriff gemäß Art. 4 Abs. 1 Nr. 44 MiFID II[46] in nationales Recht um. Darauf aufbauend müssen folgende Kriterien gleichzeitig erfüllt sein, damit ein *Token* als Wertpapier nach § 2 Abs. 1 WpHG gilt:

- Übertragbarkeit des *Token*
- Handelbarkeit des *Token* seiner Art nach auf den Finanzmärkten
- Verkörperung von mitgliedschaftlichen Beteiligungs- oder schuldrechtlichen Vemögensrechten im *Token*
- keine Einordnung des *Token* als reines Zahlungsinstrument

Über diese Voraussetzungen hat die BaFin die Öffentlichkeit bereits mit ihrem Hinweisschreiben vom 20. Februar 2018[47] detailliert informiert, so dass es hier bei einer Darstellung der Kernaspekte bleiben kann:

So setzt die Übertragbarkeit der *Token* voraus, dass der *Token* in technischer Hinsicht überhaupt auf andere Nutzer übertragen werden kann. Dabei muss der *Token* „seiner Gattung nach" übertragbar sein, also bei Übertragung auf Dritte in seinem wesentlichen rechtlichen Gehalt beziehungsweise seinem technischen Wesen nach unverändert bleiben. Was gegen eine gattungsmäßige Übertragbarkeit im Sinne der Wertpapiereigenschaft sprechen kann, sind Beschränkungen bei der Zahl möglicher Übertragungen und die Übertragung nur durch bestimmte, insoweit privilegierte Nutzer.

Für die Handelbarkeit der *Token* ist gattungsmäßige Standardisierung entscheidend. Verkörpern *Token* jeweils individuell unterschiedliche Rechte, mögen die *Token* übertragbar sein, ihre Handelbarkeit hingegen ist dann in der Regel nicht gegeben. *Token* müssen im Geschäftsverkehr nach Art und Zahl bestimmbar, also vertretbar sein. Die Verwahrfähigkeit der *Token* ist dagegen, ausgehend vom Wortlaut der Norm, keine Voraussetzung für ihre Handelbarkeit. Die Handelbarkeit muss auf Finanzmärkten gegeben sein. Dabei reicht die Möglichkeit des Handels aus, ein tatsächlicher Handel ist nicht erforderlich. Zentral wie dezentral organisierte Kryptotoken-Handelsplattformen sind hierfür grundsätzlich als Finanzmärkte anzusehen.

Der *Token* muss ein aktienähnliches mitgliedschaftliches Recht oder ein anderes vermögensmäßiges Recht schuldrechtlicher Natur verkörpern, das den in § 2 Abs. 1 WpHG genannten Beispielen für übertragbare Wertpapiere, insbesondere Anleihen oder Schuldtiteln, hinreichend vergleichbar sein muss. Gerade im Hinblick auf die oft hybride Natur vieler als Utility-Token ausgeflaggten *Token* wird im Einzelfall darauf zu achten sein, dass noch ein Finanzinstrument vorliegt und kein Instrument, das stark überwiegend der Realwirtschaft zuzuordnen ist. Ein überwiegend realwirtschaftlicher Bezug kann insbesondere dann fraglich sein, wenn mit den *Token* noch keine der versprochenen Waren oder Dienstleistungen bezogen werden können, da diese erst noch entwickelt werden müssen. In diesen Fällen hängt es unter anderem von den Anstrengungen der Emittentin ab, ob die in dem *Token* und begleitenden Materialien in Aussicht gestellte Funktionalität sich realisiert. Dadurch dient der *Token* schwerpunktmäßig Finanzierungszwecken, was für das Vorliegen eines Finanzinstruments sprechen kann, wenn ansonsten wertpapierähnliche Rechte in dem *Token* verkörpert sind.

Die Verkörperung mitgliedschaftlicher Rechte liegt insbesondere dann nahe, wenn der *Token* eine Form von Beteiligung an einem verbandsmäßig organisierten Unternehmen vermittelt, so dass sich Ähnlichkeit mit der Aktie aufdrängt.[48] Auch Konstruktionen, die ähnlich einem Hinterlegungsschein für eine Aktie oder ein aktienähnliches Papier nur einen schuldrechtlichen Anspruch auf die Ausübung mitgliedschaftlicher Rechte vermitteln, können mitgliedschaftliche Rechte verkörpern.

Eine Verkörperung vermögensmäßiger Rechte liegt nahe, wenn die mit dem *Token* verknüpften Rechtspositionen einem Schuldtitel angenähert sind, indem etwa

46 RL (EU) 2014/65, ABl. L 173/349.

47 BaFin, Initial Coin Offerings: Hinweisschreiben zur Einordnung als Finanzinstrumente, www.bafin.de/dok/10506450, abgerufen am 10.07.2018.

48 Roth, in: Hirte/Möllers, Kölner Kommentar zum WpHG, 2. Aufl. 2014, § 2 Rdn. 48.

schuldrechtliche Ansprüche gegen die Emittentin des *Token* oder Dritte bestehen. Dafür ist allerdings erforderlich, dass der schuldrechtliche Anspruch grundsätzlich an den *Token* geknüpft ist und nur mit diesem übertragen werden kann.

Schließlich darf der *Token* nicht als reines Zahlungsinstrument eingeordnet werden: Als Zahlungsinstrument zählen insbesondere Zahlungsmittel wie Bar-, Buch- und elektronisches Geld, aber auch sonstige Instrumente, mit denen bestimmungsgemäß ein Zahlungsvorgang eingeleitet wird.[49] Erfüllt ein *Token* die Voraussetzungen eines Zahlungsinstruments, ist der *Token* als dann rein elektronisches Zahlungsmittel von dem Wertpapierbegriff des WpHG ausgeschlossen. Insbesondere in diesen Fällen greift die Einordnung als Rechnungseinheit nach § 1 Abs. 11 Satz 1 Nr. 7 KWG.

Ein als Wertpapier zu qualifizierender *Token* führt dann auch zur Anwendbarkeit der auf Wertpapiere zugeschnittenen Kapitalmarktregulierung. Zu nennen sind hier etwa mögliche Prospektpflichten nach § 3 Abs. 1 WpPG beziehungsweise Art. 3 Abs. 1 Prospektverordnung[50] im Falle eines öffentlichen Angebots, die Anwendbarkeit der Organisations- und Verhaltenspflichten[51] sowie die Möglichkeit der Produktintervention nach dem WpHG[52]. Weiterhin zu beachten wären die Regelungen zu den Handelspflichten und zur Marktüberwachung nach der MiFIR[53] und auch die Regelungen zum Marktmanipulationsverbot, zum Verbot von Insidergeschäften, zu den Ad-hoc-Pflichten für Emittenten und den Pflichten für Finanzanalysen aus der MAR, soweit die zusätzlichen Anforderungen des Art. 2 MAR erfüllt sind, die Wertpapiere also insbesondere auf einem geregelten Markt, einem multilateralen oder organisierten Handelssystem gehandelt werden. Das wäre etwa der Fall, wenn ein Kryptohandelsplatz im Anwendungsbereich der Verordnung als *Multilateral Trading Facility* (MTF) oder *Organised Trading Facility* (OTF) zugelassen würde. Nicht zuletzt unterfallen gewerbsmäßig oder in einem kaufmännischem Umfang betriebene Geschäfte mit Wertpapieren den Erlaubnispflichten nach KWG und führen dadurch auch zu der Verpflichteteneigenschaft nach § 2 GwG.

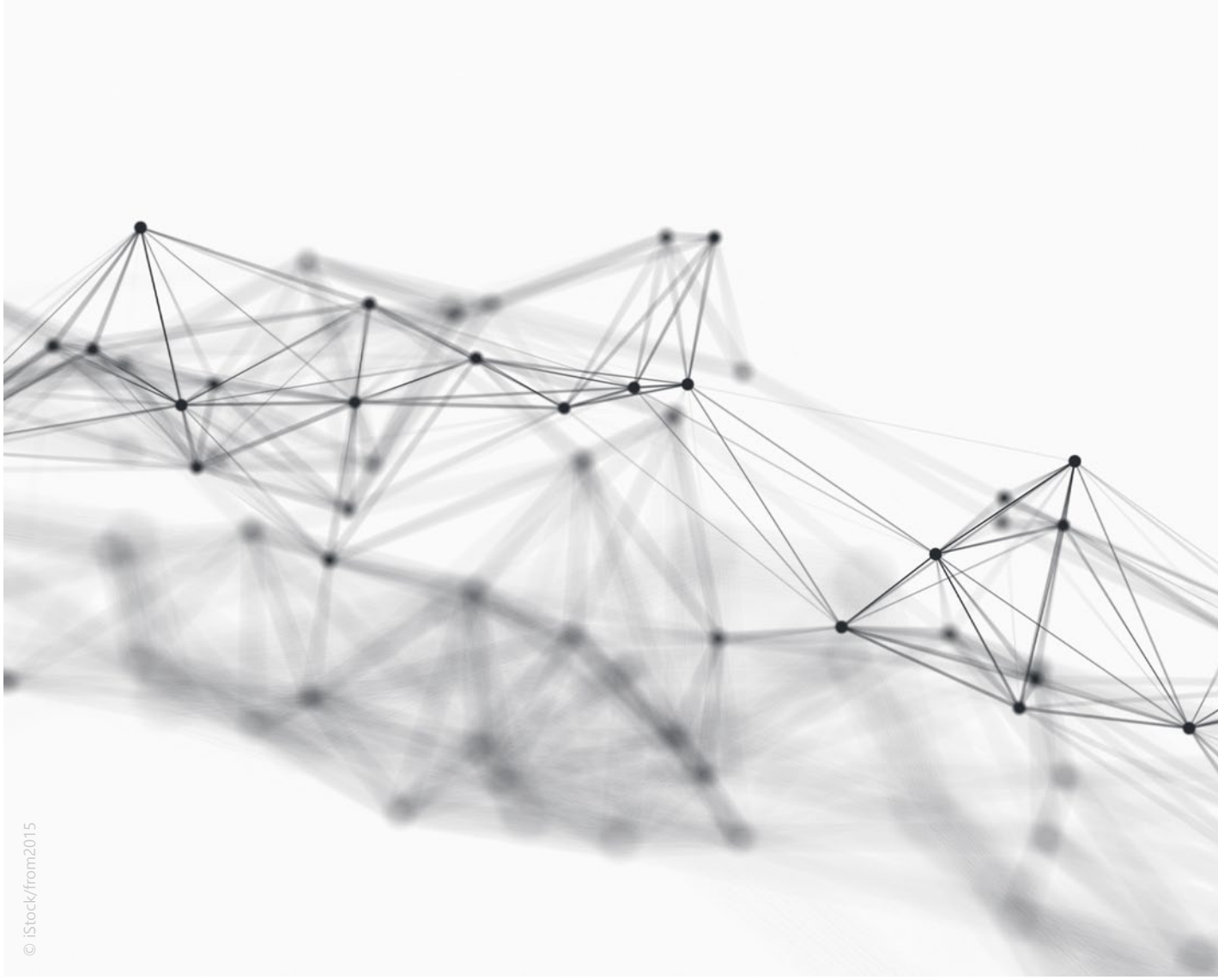
4.1.3 Utility-Token

Bei reinen *Utility-Token* (*App-Token*, Nuzungstoken, Verbrauchstoken) steht die alleinige Nutzung zum Bezug einer realwirtschaftlichen Dienstleistung im Vordergrund und nicht eine finanzielle Gegenleistung. Bei *Utility-Token* handelt es sich nicht um E-Geld, wenn keine Drittakzeptanz oder eine Ausgabe nur gegen andere *Payment-Token* (etwa Bitcoin und Ether) erfolgt. Bei reinen Nutzungstoken spricht zudem viel dafür, dass die Ausgabe auch keine Erlaubnispflichten nach dem KWG, ZAG oder KAGB auslöst. Zudem scheidet bei solchen *Token* regelmäßig auch die Einstufung als Finanzinstrument nach dem KWG aus, so dass eventuelle handelsbezogene Dienstleistungen ausschließlich mit diesen *Token* auf dem Sekundärmarkt keine Erlaubnispflichten nach sich ziehen.

Reine Nutzungstoken sind, anders als virtuelle Währungen, auch nicht als Zahlungsmittel konzipiert und qualifizieren sich daher auch nicht als Rechnungseinheiten; sie lassen sich dann auch in aller Regel nicht unter den Tatbestand anderer Finanzinstrumente nach § 1 Abs. 11 KWG fassen. Wegen der vielen Mischformen, also *Token*, die sowohl Elemente eines Nutzungstokens als auch die einer virtuellen Währung oder eines wertpapierähnlichen *Tokens* aufweisen, bedarf es jedoch oft einer vertieften Prüfung.

Kommt nämlich dem vermeintlichen *Utility-Token* im Rahmen des Angebots des Emittenten auch die Funktion eines Zahlungsmittels zu, ist eine Qualifizierung als Rechnungseinheit und damit Finanzinstrument nach KWG wieder naheliegend. Aus aufsichtsrechtlicher Sicht ist die Kategorie der *Utility-Token* das Ergebnis einer Negativabgrenzung zu den vorrangig zu prüfenden Kategorien der Zahlungstoken und der wertpapierähnlichen *Token*, die aufsichtsrechtliche Pflichten auslösen.

49 BaFin, Merkblatt Finanzinstrumente, a.a.O. (Fn. 45).
50 Verordnung (EU) Nr. 2017/1129, ABl. L 168/12.
51 Zu den Verhaltensregelungen und weitere Verweisen, siehe BaFin-Journal Mai 2018, Seite 18ff.
52 www.bafin.de/dok/10334186.
53 Verordnung (EU) Nr. 600/2014, ABl. L 173/84.



4.1.4 Initial Coin Offerings

ICOs sind sowohl wirtschaftlich als auch organisatorisch von *Initial Public Offerings* (IPOs) zu unterscheiden.[54] ICOs werden vereinzelt auch als *Token Generating Event* (TGE) bezeichnet. Bei einem ICO werden *Token* verkauft beziehungsweise versteigert. Kernidee von ICOs ist es, Gelder von Dritten für eine Idee oder ein Geschäftsmodell einzusammeln.

Oft finden sich bei ICOs *Whitepaper*, die einen Überblick über das geplante Vorhaben geben sollen, aber regelmäßig nicht an die Struktur, Vergleichbarkeit und Aussagekraft von Wertpapierprospekten nach WpPG heranreichen. Der weitere Kontakt mit den Emittenten findet dann häufig über diverse Onlinekanäle wie etwa die Webseite, Telegram-Channel und Slack statt. Technisch nutzen viele ICOs *Smart Contracts* von Ethereum, der nach Marktkapitalisierung derzeit zweitgrößten *Blockchain* nach Bitcoin. In solchen *Smart Contracts* werden dann die *Token* verwaltet, die im Rahmen des ICOs versteigert oder veräußert wurden.

Ökonomisch bestehen bemerkenswerte Unterschiede zwischen der Kapitaleinsammlung über klassische eigen- oder fremdkapitalbasierte Refinanzierungsinstrumente und einem idealtypischen ICO, der Elemente der hier dargestellten Blockchain-Ökonomie abbildet. Kryptotoken können den durch die Beiträge Dritter bestimmten Wert von dezentralen Netzwerken unmittelbar abbilden, während klassische (Unternehmens-) beteiligungen zunächst den Wert des initiierenden Unternehmens abbilden und nur mittelbar den Wert des von ihm initiierten (nicht notwendig betriebenen) dezentralen Netzwerks. Bei dezentral angelegten Netzwerken kommt es ab einem gewissen Zeitpunkt auf die Bemühungen der beteiligten Community an und weniger auf die der Initiatorin.[55] ICOs ermöglichen auch privaten Investoren Zugang zu *Venture-Capital*

54 Conley, Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings, http://www.accessecon.com/Pubs/VUECON/VUECON-17-00008.pdf, abgerufen am 10.07.2018.

55 Voraussetzung ist hier aber, dass das Netzwerk schon funktional ist und es sich nicht nur um ein Versprechen der Emittentin handelt.

ähnlichen, dabei liquideren, zugleich aber riskanteren Investitionsgelegenheiten. Schließlich können ICOs unter Einsatz von *Smart Contracts* Transaktionskosten optimieren – und zwar durch automatisierte, nichtdiskretionäre, dezentrale und ohne weiteres grenzüberschreitende Abwicklung vertraglicher Abreden. Die Desintermediationseffekte der Blockchain-Technologie – als Basis der ICOs – lindert ferner Konzentrationseffekte in intermediärbasierten Plattformökonomien und sorgt für Wettbewerbsdruck auf diese etablierten Intermediäre.[56]

Aufsichtsrechtlich ist zu unterscheiden zwischen der Erstemission der *Token*, dem eigentlichen ICO, und dem späteren Handel mit den *Token* auf dem Zweitmarkt. Die aufsichtsrechtliche Einstufung des *Token* hat dann Auswirkungen auf mögliche Verpflichtungen sowohl bei der Emission (etwa Prospektpflicht) als auch auf mögliche Pflichten Dritter, die an der Emission und dem Zweitmarkthandel beteiligt sind. Besonders hervorzuheben sind hier die oben erläuterten Erlaubnispflichten insbesondere für Zweitmarktgeschäfte wie den Betrieb von Kryptohandelsplätzen und Geschäfte an der Schnittstelle zu realem Geld. Ein Beispiel hierfür ist der Betrieb von Tauschautomaten, da das Betreiben dieser Geschäfte in Deutschland ohne vorherige Erlaubnis strafbewehrt ist. Dagegen kommt es für die eigene Emission im Rahmen eines ICOs nicht entscheidend auf die Rechtsnatur der emittierten *Token* an, da das Aufsichtsrecht ein weitgehendes Emittentenprivileg einräumt; die Emission eigener Refinanzierungsintrumente durch Unternehmen der Realwirtschaft löst für sich genommen meist keine Erlaubnispflicht nach dem KWG aus.

ICOs sind von einer anderen häufigen Erscheinungsform, dem *Airdrop*, zu unterscheiden. Bei einem *Airdrop* werden kostenlose *Token* von Blockchainprojekten verteilt. Wer bei *Airdrops* kostenlose *Token* erhalten will, muss meist *Token* des entsprechenden Blockchainprojekts halten. Nicht selten wird allerdings auch eine Gegenleistung in Form von *Likes* oder *Retweets* verlangt, damit die *Airdrop-Token* ausgeschüttet werden. *Airdrop-Token* unterscheiden sich meist nicht von regulären *Token* und können frei gehandelt werden. Ziel von *Airdrops* ist es, die Bekanntheit, das Handelsvolumen und langfristig den Wert des zugehörigen Kryptotokens zu steigern.

ICOs sind nach Ansicht der BaFin für Anleger hochspekulative Kapitalanlagen. Anleger sollten von einer hohen Volatilität ausgehen und einen potenziellen Totalverlust ihrer Investition berücksichtigen, besonders bei frühen Experimentalprojekten. Wenn Anleger *Token* bei einem ICO erwerben, befinden sich die Emittenten meist nicht in Deutschland. Es greifen dann kein deutscher Verbraucherschutz und kein Schutz personenbezogener Daten. Die Dokumentation durch *Whitepaper* ist meist unzureichend und verwirrend und erreicht nicht das Informationsniveau von Wertpapierprospekten nach dem WpPG. Um Risiken von ICOs beurteilen zu können, ist ein tiefes, insbesondere technisches Verständnis notwendig. ICOs finden oft im nicht regulierten Bereich des Finanzsektors statt und nutzen Jurisdiktionen mit laxerer Regulierung. ICOs weisen zudem eine strukturell hohe Anfälligkeit für Missbrauch und Betrug auf.[57]

Um dieser Risikosituation gerecht zu werden, hat die BaFin am 9. November 2017 eine Verbraucher-Warnung[58] und einen begleitenden Artikel im BaFinJournal[59] veröffentlicht. Zudem hatten sich Berichte über Schadensmeldungen im Kontext von ICOs gehäuft, und es gab deutliche Anzeichen für eine Marktüberhitzung. Selbst aus der Kryptoszene waren Warnungen zu hören. Der BaFin lagen zudem Erkenntnisse über technische Unzulänglichkeiten einzelner ICO-Konzepte vor.

Die Primär- oder Hauptrisiken mit unmittelbarem Bezug[60] zu Kryptotoken umfassen insbesondere 1) Marktliquiditäts- und Volatilitätsrisiken, 2) Kontrahenten- und

56 Klöhn/Parhofer/Resas, Initial Coin Offerings (ICOs) – Markt, Ökonomik und Regulierung, in: Zeitschrift für Bankrecht und Bankwirtschaft 2018, 89ff., 93f. m.w.N.

57 Pressemeldung Marktwächter Finanzen, Neue Kryptowährungen sind hochriskante Geldanlagen, http://ssl.marktwaechter.de/pressemeldung/neue-kryptowaehrungen-sind-hochriskante-geldanlagen, abgerufen am 03.7.2018.

58 www.bafin.de/dok/10181964.

59 Vgl. BaFinJournal November 2017, Seite 15.

60 Auf die mittelbaren Leverage-Risiken, die bei Einsatz von Kryptotoken als Basiswert für Derivate entstehen oder durch Erwerb von Kryptotoken unter Einsatz von Fremdkapital wie Darlehen, wird hier nicht weiter eingegangen.

Projektrisiken sowie 3) technische und operationelle Risiken (einschließlich Cybersicherheitsrisiken). Diese Hauptrisiken beziehen sich sowohl auf spezifische Merkmale von Kryptotoken und deren aktuelle Nutzung als auch auf bekanntere mikrofinanzielle Risiken im Zusammenhang mit Marktliquidität, Volatilität, *Leverage* usw.[61]

- Marktliquiditäts- und Volatilitätsrisiken: Im Bezug auf Kryptotoken ist besonders zu beachten, dass illiquide oder flache Marktstrukturen die Fähigkeit zum Kauf oder Verkauf von Kryptotoken ohne Einfluss auf die Preise beeinträchtigen. Auch die hohe Volatilität der Marktpreise lässt daran zweifeln, dass Kryptotoken für Privatanleger geeignet sind und sich für Zahlungen und Abrechnungen verwenden lassen. Hinweise zu spezifischen Risiken können das Handelsvolumen, die Preise, die Preisvolatilität, die Zahl der Nutzer, die *Bid-Ask-Spreads*, die Preisspreads zwischen Börsen und die Kosten für den Abschluss von Geschäften geben.
- Kontrahenten- und Projektrisiken: Das Projektrisiko von Kryptotoken aus ICOs und den damit finanzierten Projekten könnte die Positionen der Kryptotoken-Inhaber (Investoren) beeinflussen, da der Wert und die Stabilität der Kryptotoken bei vielen Projekten maßgeblich von dem Projektteam abhängen, das hinter den Kryptotoken oder dem ICO steht. So könnte es vorkommen, dass das Projekt hinter einem ICO nicht zustande kommt, was die Kryptotoken letztlich wertlos machte. Diese Risikoklasse ist insbesondere im Kontext von ICOs relevant, da die Gesamtgröße des ICO-Marktes im Verhältnis zum gesamten Kryptotoken-Markt derzeit noch gering ist. Darüber hinaus geht von Kryptotoken-Brokern, Krypto-Handelsplattformen, Wallet- Providern und anderen Intermediären für Inhaber von Kryptotoken auch ein Gegenparteienrisiko aus.
- Technische und operationelle Risiken (einschließlich Cybersicherheitsrisiken): Die Blockchain-Technologie kann künftig grundsätzlich eine Reihe von Vorteilen bieten. Allerdings bergen Kryptotoken, insbesondere solche, die Teil dezentraler Projekte sind und daher mit begrenzt effektiven Governance-Strukturen arbeiten, auch besondere technische und operative Risiken. Dazu gehört die Anfälligkeit für Diebstahl und Betrug. Cyberangriffe, die Finalität von Transaktionen, schlechte Skalierbarkeit und lange Verzögerungszeiten können ebenfalls operationelle Risiken darstellen. Solche Risiken, insbesondere die überproportional hohe Abhängigkeit von funktionierenden IT-Infrastrukturen, bestehen auch bei Dienstleistern wie Kryptotoken-Handelsplattformen.

Die vorangegangene Betrachtung hat gezeigt, dass, abhängig von der Ausgestaltung im Einzelfall, nicht alle *Token* der Kapitalmarktregulierung in einer Weise unterfallen, dass diese Risiken so erfasst werden, wie dies bei klassischen Kapitalmarktinstrumenten der Fall ist. Daher gilt es für private wie institutionelle Investoren, aber auch im Sinne der Finanzstabilität und -integrität, Indikatoren und Transmissionskanäle dieser Risiken in das Finanzsystem zu beobachten.[62]

61 Zu Risiken, die spezifisch auf die Situation bei einem ICO abstellen, vgl. die ausführliche Darstellung in Klöhn/Parhofer/Resas, a.a.O. (Fn. 56), Seite 95ff.

62 FSB, FSB report sets out framework to monitor crypto-asset markets, abgerufen am 27.07.2018.

5 Zusammenfassung

Der Kryptotoken-Markt als Ganzes weist eine hohe Innovationsgeschwindigkeit, starke Informationsasymmetrien und Lücken in der Datenverfügbarkeit auf. Dies bedeutet sowohl für nationale Aufsichtsbehörden wie die BaFin als auch für europäische Aufsichtsbehörden und internationale Standardsetzer, dass sie sich weiter intensiv mit dem Thema beschäftigen und die Entwicklung verfolgen müssen.

Mehr als 1.600 Kryptotoken werden zurzeit auf Marktplätzen gehandelt, wobei lediglich fünf Kryptotoken den Großteil des Transaktionsvolumens ausmachen. Zwar sind die Preise für Kryptotoken seit Ende 2017 deutlich gesunken, was zu einem deutlichen Rückgang der Marktkapitalisierung geführt hat. Ende Juni 2018 beträgt diese nur noch knapp ein Drittel des Höchstwertes aus Januar 2018. Zugleich ist aber eine deutliche Zunahme der Zahl und des Volumens an ICOs festzustellen: Das Volumen ist knapp um das Sechsfache höher als im Vergleich zu 2017 (3,9 Mrd. US-Dollar), wenn man die Zahlen des ersten Halbjahres auf das Gesamtjahr 2018 extrapoliert; die Zahl ist – bei Extrapolation der ersten Jahreshälfte auf das Gesamtjahr 2018 – knapp um das Fünffache höher als im Vergleich zu 2017 (210 ICOs). Weltweit wurden in der ersten Jahreshälfte 2018 bereits mehr als elf Mrd. US-Dollar im Rahmen von 489 ICOs eingesammelt.[63] Im Vergleich zum globalen Finanzsystem sind die Märkte für Kryptotoken aber nach wie vor klein und beeinträchtigen die Finanzstabilität daher noch nicht.[64]

63 CoinSchedule, Cryptocurreny ICO Stats 2018, http://www.coinschedule.com/stats.html, abgerufen am 25.06.2018.
64 FSB, a.a.O. (Fn. 62).

Angesichts der Wachstumsraten kann im Hinblick auf ICOs und die dadurch geschaffenen Kryptotoken durchaus von einem Hype gesprochen werden. Allerdings ist davon auszugehen, dass die Phänomene Kryptotoken und ICO auch nach einer Beruhigungsphase bestehen bleiben, denn ICOs können neben den oben bereits beschriebenen Vorteilen absehbar zu einer bedeutenden Finanzierungsquelle werden, insbesondere im Rahmen der Frühphasenfinanzierung junger Unternehmen.[65]

Darüber hinaus sind die Verbindungen zur traditionellen Finanzindustrie bislang begrenzt. Trotz Einführung von Kryptotoken-Futures sind die gehandelten Volumina und Positionen der Finanzinstitute im Vergleich zu ihren Engagements an den Märkten für andere Vermögenswerte nach wie vor gering.

Der Kryptotoken-Raum entwickelt sich auch qualitativ rasant weiter. So haben einige Marktteilnehmer Interesse an der Einführung von Kryptotoken-Exchange-Traded-Funds (ETFs) bekundet, die das Potenzial haben, das Kryptotoken-Risiko für Privatkunden schnell zu erhöhen, indem sie die technologischen Barrieren für das direkte Halten von Kryptotoken senken.

Je mehr Wissenschaft, Politik, internationale Standardsetzer und Aufsichtsbehörden sich mit diesem Thema beschäftigen, desto mehr Rechtssicherheit kehrt in den Markt ein – trotz zahlreicher verbleibender Fragen. Zudem sind auch die aufgeführten positiven Effekte einzelner Erscheinungsformen wie ICOs bei allen Risiken nicht zu verkennen.

Die derzeit geringe Bedeutung dieses Marktes für die Finanzstabilität kann daher noch kein abschließender Befund sein.[66] Im Hinblick auf die regulatorische und aufsichtliche Erfassung aller Facetten der Blockchain-Ökonomie besteht zwar gerade in Deutschland kein unreguliertes Wild-West-Szenario, aber auch keine vollständig eingehegte Aufsichts- und Regulierungslandschaft.

Der Preis für die risikoadäquate und technologieunabhängige Regulierung ist ein vergleichsweise hoher anfänglicher Zeitaufwand bei der Einführung neuer Geschäftsmodelle. Das individuelle Interesse der Anleger an einer möglichst kurzfristig und komplikationslos zu erzielenden Investitionsrendite und das Interesse der Emittenten an einer schnellen Einsammlung fremder Mittel zur Verwendung für eigene gewerbliche Zwecke[67] sind aber seitens der BaFin stets in Einklang zu bringen mit dem übergeordneten, dem Allgemeinwohl verpflichteten Ziel eines integren und vertrauenswürdigen Finanzmarktes. Dadurch können sich aber nachhaltige, durchdachte und damit vertrauenswürdige Finanzinnovationen durchsetzen und letztlich auch individuell auszahlen. Trotz der unbestrittenen Erschwernisse durch die Klärung aufsichtsrechtlicher Fragen vor Markteinführung eines Geschäftsmodells hat sich dieses regulatorische Grundkonzept auch bei den Finanzinnovationen der vergangenen Jahrzehnte im Grundsatz bewährt. Die vom Einzelfall losgelöste strategische Betrachtung der vielfältigen Anwendungen der Blockchain-Technologie, etwa durch *Token*, stellt zugleich sicher, dass aus Sicht aller öffentlichen wie privaten Interessen unnötige oder überholte regulatorische Hindernisse adressiert werden können.

Über die Festigung von Rechtssicherheit im Wege einer fortgesetzten Marktinformation und einer gezielten, international abgestimmten Analyse möglicher Regulierungsdefizite können auch hier noch Fortschritte erwartet werden.

65 Weitnauer, Initial Coin Offerings, rechtliche Rahmenbedingungen und regulatorische Grenzen, in: Bank- und Kapitalmarktrecht 6/2018, Seite 231ff.; 236; Zickgraf, Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, in: Die Aktiengesellschaft 2018, Seite 293ff., 307.

66 Vgl. Ausschuss für Finanzstabilität (AFS), Fünfter Bericht an den Deutschen Bundestag, Juni 2018, Seite 42.

67 Bislang ist noch kein Fall eines ICOs bekannt, bei dem nicht auch Gewinnerzielungsinteressen der Initiatoren eine Rolle spielen. Gerade im Kontext der Blockchain-Technologie wird dieser Umstand oft verstellt von marketingorientierten Ausführungen an Politik und Investoren, dass die Investition in einen ICO einem höheren Gut diene – etwa der Etablierung dezentraler Plattformen ohne Mittelsmänner. Tatsächlich ist es auch Merkmal einer Blockchain-Ökonomie, dass es zur Gewinnerzielung keiner Mittelsmänner oder zentraler Kontrolle der Plattform bedarf, wenn man in der Erwartung einer späteren Wertsteigerung nur genügend der zunächst kostenlos geschaffenen *Token* für sich behält.

V

In einer globalisierten Finanzwelt, in der immer mehr Menschen digital bezahlen, Geld transferieren und ihre Geldanlage online bestreiten, haben IT-Governance und Informationssicherheit für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Unternehmen mit Kapital und Liquidität. Für die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) war es daher ein logischer Schritt, ihre Anforderungen auf diesem Gebiet zu konkretisieren.

Digitalisierung und Informationssicherheit im Fokus aufsichtlicher Anforderungen

Autor

Dr. Jens Gampe,
Referat Grundsatz IT-Aufsicht und Prüfungswesen, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

1 Einleitung

Informationstechnik (IT) ist heute in der Finanzwelt nicht mehr nur Nebenbedingung, um Erträge zu generieren, sie ist inzwischen – und das macht sie auch angreifbar – Basisinfrastruktur für sämtliche bankfachlichen, aber auch alle nichtbankfachlichen Prozesse. Darauf hat auch BaFin-Präsident Felix Hufeld hingewiesen, etwa bei der BaFin-Informationsveranstaltung „IT-Aufsicht bei Banken" am 16. März 2017.[1] Darüber hinaus ist IT-Sicherheit auch ein gesellschaftlich relevantes Thema.

Beide Aspekte, IT als Grundlage für das Wirtschaften entlang aller Wertschöpfungsketten im Finanzsektor und der Verweis, dass ohne Informationssicherheit[2] kein nachhaltiges und gesellschaftlich akzeptiertes Geschäft möglich sei, waren für die BaFin ausschlaggebend dafür, die Bankaufsichtlichen Anforderungen an die IT (BAIT) zu entwickeln – gemeinsam mit der Deutschen Bundesbank und in Abstimmung mit Vertretern der Kreditinstitute und ihrer Verbände. Am 6. November 2017 hat die BaFin die BAIT[3] veröffentlicht. Mit den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT)[4], die die BaFin am 2. Juli 2018 publiziert hat, sind vergleichbare Anforderungen an die Versicherungswirtschaft geschaffen worden.

BAIT und VAIT sind prinzipienorientiert und proportional gestaltete Regelwerke, deren Zweck darin besteht, die bislang eher allgemein gehaltenen Anforderungen der Aufsicht an die IT zu konkretisieren und transparenter zu machen.

1 www.bafin.de/dok/9045758.

2 DTCC & Oliver Wyman, Large-scale cyber-attacks on the financial system – A case for better coordinated response and recovery strategies, http://www.oliverwyman.com/our-expertise/insights/2018/mar/large-scale-cyber-attacks-on-the-financial-system.html, abgerufen am 08.05.2018.

3 Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT).

4 Rundschreiben 10/2018 (VA) – Versicherungsaufsichtliche Anforderungen an die IT (VAIT).

2 Wandel der Anforderungen an die IT im Finanzsektor

Der Wertschöpfungsprozess der Banken besteht seit jeher im Wesentlichen aus der Verarbeitung von Informationen. Die Digitalisierung ist also für die Institute nicht neu. Die Digitalisierung der Bankgeschäfte vollzog sich in der Vergangenheit jedoch maßgeblich im Innern der Institute und war lange Zeit – trotz ihrer Bedeutung insbesondere im Zahlungsverkehr – für die meisten Kunden kaum wahrnehmbar.

Erste Onlinebanking-Angebote (Stichwort „BTX“[5]) für Kunden kamen bereits vor mehr als 30 Jahren auf. Aber erst in den vergangenen zehn bis 15 Jahren haben sich der bargeldlose Zahlungsverkehr – auch im Rahmen des zunehmend intensiver genutzten Online-Bankings – und das Online-Brokerage im Privatkundengeschäft etabliert. Mit konkurrenzfähigen Direktbanken und den ersten App-basierten volldigitalisierten Instituten ist nun die nächste technische Evolutionsstufe in der Interaktion mit Kunden erreicht.

Digitalisierung im *Banking* heißt aber auch, Geschäfts- und IT-Prozesse mit Hilfe relevanter Daten und geeigneter IT-Systeme (Hard- und Softwarekomponenten) zu unterstützen und zu automatisieren – über alle Kundenkanäle, die gesamte Informationskette im Unternehmen und über definierte Schnittstellen mit Dritten hinweg.[6] Hierbei kommt es insbesondere auf eine intelligente Vernetzung von Geschäftsprozessen an, die sich in vielen Fällen auch über mehrere Unternehmenseinheiten erstrecken. Nicht zu vergessen ist auch das zunehmend intensivere Zusammenwirken mit Unternehmen, die für die Institute externe IT-Dienstleistungen in mehr oder minder großem Umfang erbringen.

Die aufsichtliche Überwachungs- und Prüfungspraxis zeigt, dass es vielen Banken noch immer Probleme bereitet, mehrere beziehungsweise unterschiedlich digitalisierte Geschäftsprozesse technisch angemessen miteinander zu verknüpfen. Dies ist jedoch für eine Digitalisierung, die das Geschäft zielorientiert unterstützen soll, entscheidend. Es genügt nämlich nicht, einzelne Prozesse zu digitalisieren oder nur in Teilbereichen digitale Geschäftsmodelle einzuführen. Der technologische Fortschritt erzwingt eine sehr viel stärkere Ausrichtung an Innovation und eine permanente Anpassung an das Kundenverhalten, das sich dynamisch verändert.[7]

Somit bringt die Digitalisierung neben den allgegenwärtigen und weiter zunehmenden Informations- und Cybersicherheitsrisiken auch Risiken strategischer Natur für die Banken und ihre IT-Dienstleister mit sich, weil sie die Wertschöpfungsketten im Finanzdienstleistungssektor verändert.[8] Derzeit zeichnen sich bei der Digitalisierung im Bankensektor verschiedene Trends[9] ab.

Nachfolgend werden einige technologische (Weiter-)Entwicklungen kurz dargestellt:

Digitalisierungsinitiativen an der Kundenschnittstelle
In klassischen Filialbanken wurden zwar schon früh Online-Banking-Angebote entwickelt, deren Umsetzung wurde aber zumeist nur halbherzig begleitet, da der Fokus darauf gerichtet war, dass die Kundschaft die Filialen nutzte. Inzwischen hat zwar die Qualität der digitalen Angebote erheblich zugenommen, diese werden jedoch in vielen Fällen noch immer unzureichend mit dem klassischen Filialgeschäft abgestimmt, obwohl die meisten Kunden inzwischen Angebote über alle Vertriebskanäle hinweg[10] erwarten.

5 Bildschirmtext.

6 Röseler, Banking wird sich ganz radikal ändern, Treiber des Wandels ist die Digitalisierung, in: Zeitschrift für das gesamte Kreditwesen, Nr. 7/2018, Seite 25 ff.

7 COREtransform: White Paper – Primat des Technologischen – Regulatorik im Spannungsfeld zwischen Gestalten und Verwalten, https://transform.core.se/de/about/insights/knowledge-work/white-paper/, abgerufen am 11.05.2018.

8 BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, Seite 7 ff. und Seite 64 ff., www.bafin.de/dok/10985478, abgerufen am 11.05.2018.

9 Deutsche Bank Research, Fintech reloaded – Die Bank als digitales Ökosystem, https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000443890/Fintech_reloaded_%E2%80%93_Die_Bank_als_digitales_%C3%96kosyste.pdf, abgerufen am 11.05.2018.

10 Stollarz, Digitalisierung in der Finanzbranche ist kein Selbstzweck, in: Börsen-Zeitung online, 28.04.2018, Seite B5.

In diese Lücke stoßen seit einigen Jahren zunehmend Direktbanken, Fintechs[11] und Crowdfunding-Plattformen, die oft nur einen spezifischen Teil des Bankgeschäfts anbieten. Die zunehmende Popularität dieser innovativen Anbieter hat den Wettbewerbs- und Investitionsdruck auf die etablierten Player im Bankensektor deutlich erhöht.[12] Wenn sie sich in diesem Umfeld behaupten wollen, müssen sie mehr tun als in Technik zu investieren – etwa in die Implementierung von mobilen Apps und Omnichannel-Plattformen. Die Banken müssen auch ihre Ablauforganisation und ihre Steuerungsmechanismen zügig an die neuen Entwicklungen anpassen.

11 Eine allgemeingültige Definition des Begriffs Fintechs existiert bisher nicht. Als Kombination aus den Worten *Financial Services* und *Technology* versteht man unter Fintechs gemeinhin junge Unternehmen, die mit Hilfe technologiebasierter Systeme spezialisierte und besonders kundenorientierte Finanzdienstleistungen anbieten.

12 Deutsche Bank Research, Kommentar – Start-ups beflügeln Märkte mit digitalen Technologien (Fintech #7), https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000447700/Start-ups_befl%C3%BCgeln_M%C3%A4rkte_mit_digitalen_Technolog.PDF, abgerufen am 11.05.2018.

Prozessdigitalisierung

Mit der zunehmenden Reife digitaler Technologien entstehen neue Möglichkeiten, bislang nur teilautomatisierte Prozesse weiter zu automatisieren – etwa im Kreditgeschäft (Stichwort „Kreditfabrik“) und rund um die Eröffnung von Konten (Stichwort „VideoIdent“).

Die etablierten Banken werden im Onlinegeschäft jedoch nur dann mit den neuen, digitalen Wettbewerbern konkurrieren können, wenn sie auch angrenzende Backend-Prozesse stärker automatisieren und so die Kostenstrukturen erheblich verbessern. Und auch bei der Prozessdigitalisierung reicht es nicht aus, neue Lösungen zu entwickeln. Diese Lösungen müssen zügig und wirksam in die Wertschöpfungs- beziehungsweise Prozessketten integriert werden – im Institut und institutsübergreifend.

Hinzu kommt, dass sie sich dabei vielerorts mit veralteten und/oder zu komplexen IT-Systemen auseinandersetzen müssen. Viele Institute weisen zudem erhebliche Mängel in ihrer IT-Governance auf, wie die Aufsicht

festgestellt hat. Oft werden auch im Rahmen der *Governance* getroffene Vorgaben nicht wirksam umgesetzt beziehungsweise die Operationalisierung nur unzureichend überwacht.[13]

Neue Dynamik in IT-Projekten

Was Kunden in Bezug auf die Nutzung moderner Technologien von Banken erwarten, gilt zunehmend auch für die IT-Projektorganisation und die in diesem Rahmen umgesetzte Softwareentwicklung in den Instituten und bei deren IT-Dienstleistern: Sie müssen schnell, schlank und kurzfristig anpassbar sein – kurzum: agil.

Mittlerweile organisieren nach eigenen Angaben mehr als 35 Prozent der Banken IT-Entwicklungsprojekte nach Scrum, etwa 30 Prozent setzen auf Kanban.[14] Beide agilen Softwareentwicklungsansätze bieten die Möglichkeit, Softwarebestandteile im Entwicklungsprozess noch erheblich zu verändern. Somit kann eine einsatzfähige Grundversion einer Applikation bestenfalls bereits nach wenigen Wochen zur Verfügung stehen und nicht erst nach Monaten.

Bei aller Begeisterung für innovative Softwareentwicklung sollte jedoch nicht außer Acht bleiben, dass es für einen sicheren IT-Betrieb essenziell ist, dass neben einer geeigneten funktionalen Hardware insbesondere auch Software erforderlich ist, die möglichst so entwickelt wurde, dass Sicherheitsmaßnahmen den herkömmlichen Softwareentwicklungsprozess ergänzen. Nur so kann grundsätzlich gewährleistet werden, dass ausreichend auf Sicherheit geachtet wird, unabhängig davon, ob man eine agile oder andere Vorgehensweise bei der Entwicklung wählt.[15] Dies setzt jedoch voraus, dass Sicherheit als explizite Anforderung in den Entwicklungsprozess aufgenommen wird (Stichwort „*Security by Design*") und dass ganzheitliche Sicherheitsmaßnahmen von der Initialisierung an berücksichtigt, umgesetzt, getestet und vor Produktivsetzung fachlich abgenommen werden.

Abschied vom eigenen Rechenzentrum – ist die Cloud als ‚as a Service' eine Lösung?

Bereits heute arbeiten nach eigenen Angaben über 50 Prozent der befragten Unternehmen im Finanzsektor an der Straffung ihrer Rechenzentren und der Konsolidierung ihrer IT-Infrastruktur.[16] Möglich macht dies auch die stärkere Nutzung externer Cloud-Dienste, auf die zum Beispiel Anwendungen, Plattformen und auch Sicherheitslösungen verlagert werden. Insbesondere mit As-a-Service-Konzepten[17] können Unternehmen ihre IT-Architektur sowohl standardisieren als auch beschleunigen.[18] Mit der Verlagerung der Verarbeitung teilweise hochsensibler Daten in die *Cloud* geht jedoch auch ein erhebliches Sicherheitsrisiko einher, dies betrifft sowohl die Sicherheit der IT-Systeme der *Cloud* (also die des Cloud-Betreibers) als auch die zu verarbeitenden beziehungsweise gespeicherten Daten in der *Cloud* (also die des Cloud-Nutzers).[19]

13 Vgl. hierzu Abschnitt 6., Governance – II.2. BAIT.

14 IT Finanzmagazin, 70 Prozent der Banken und Versicherer entwickeln mit agilen IT-Methoden wie Scrum oder Kanban, https://www.it-finanzmagazin.de/70-prozent-der-banken-und-versicherer-entwickeln-mit-agilen-it-methoden-wie-scrum-oder-kanban-35438, abgerufen am 11.05.2018.

15 Schild, Heise Online – Sichere Softwareentwicklung nach dem „Security by Design"-Prinzip, https://www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html, abgerufen am 11.05.2018.

16 Bain & Company, Mehr Tempo, weniger Altlasten: IT-Architektur im digitalen Zeitalter, http://www.bain.de/Images/Bain-Studie_IT-Architektur_im_digitalen_Zeitalter.pdf, abgerufen am 11.05.2018.

17 *Infrastructure as a Service* (IaaS) ist neben *Software as a Service* (SaaS) und *Platform as a Service* (PaaS) eines der drei Servicemodelle des *Cloud Computings*. Der Service beinhaltet regelmäßig die Bereitstellung von Rechenzentrumsinfrastruktur durch einen *Cloud Provider*. Der Zugriff über die Ressourcen erfolgt über private oder öffentliche Netzwerke. Zu den Komponenten der bereitgestellten Infrastruktur gehören beispielsweise Server, Rechen- und Netzkapazitäten, Kommunikationsgeräte wie Router, Switche und *Firewalls*, Speicherplatz sowie Systeme zur Sicherung und Archivierung von Daten.

18 IT Finanzmagazin, Studie zur IT-Architektur: Banken & Versicherer haben wachsende technologische Defizite, https://www.it-finanzmagazin.de/bain-studie-zur-it-architektur-banken-versicherer-haben-wachsende-technologische-defizite-45983, abgerufen am 11.05.2018.

19 com! Professional, Sicherheit in der Cloud funktioniert anders, https://com-magazin.de/praxis/cloud/sicherheit-in-cloud-funktioniert-1469946.html, abgerufen am 11.05.2018.

3 Grundsätzliche internationale aufsichtliche Anforderungen an die IT

Bereits frühzeitig hat sich die Finanzmarktaufsicht mit Anforderungen an die IT-Infrastruktur befasst und hier zunächst insbesondere Governance-Anforderungen in den Mittelpunkt gestellt. Die beim Finanzstabilitätsrat FSB (Financial Stability Board) angesiedelte Senior Supervisors Group, in der die Aufsichtsbehörden der zehn Länder vertreten sind, die die weltweit größten Banken beaufsichtigen, hat in ihrem Bericht aus dem Jahr 2010[20] die Bedeutung einer starken IT-Governance hervorgehoben und eine auch aus Sicht der BaFin zentrale Forderung aufgestellt: Die IT-Strategie muss essenzieller Teil der Geschäftsstrategie sein. Die BaFin erwartet insoweit, dass die notwendigen Anforderungen an die digitale Transformation auf geschäftspolitischen Grundlagen basieren und strategisch verankert werden, denn nur mit einem ganzheitlichen, geschäftsübergreifenden Ansatz lässt sich die IT-Architektur strategisch weiterentwickeln.

Viele IT-Regulierungsvorgaben der jüngeren Zeit sind unter anderem deshalb entstanden, weil bankinterne Prozesse, die in den technischen Systemen der Banken verarbeitet werden, (noch) nicht ausreichend integriert und automatisiert waren beziehungsweise sind, beispielsweise Datenaggregations- und Berichterstattungsprozesse, die für die Steuerung einer Bank relevant sind (Stichwort „BCBS 239"[21], die in der letzten Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) umgesetzt worden sind).

Ein weiterer Aspekt drängt im Zuge der Digitalisierung immer stärker in das Bewusstsein von Industrie und Aufsicht, nämlich die Informationssicherheit beziehungsweise die Sicherheit im Cyberraum[22] (siehe Infokasten „Definition Informationssicherheit und Cybersicherheit").

Definition

Informationssicherheit und Cybersicherheit

- Informationssicherheit umfasst den umfangreicheren Schutz von Informationen, zwar in und mit IT, aber auch ohne IT bzw. über IT hinaus.[23]
- Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.[24]

Die Cybersicherheit hat – über die Informationssicherheit hinausgehend – auch eine politische Dimension, denn es stellt sich bislang in vielen Fällen als überaus schwierig dar, nach einem Cyberangriff den realen Angreifer zu identifizieren, um anschließend wirksame Maßnahmen gegen ihn ergreifen zu können.[25]

20 Senior Supervisory Group, Observations on Developments in Risk Appetite Frameworks and IT Infrastructure, https://www.newyorkfed.org/medialibrary/media/newsevents/news/banking/2010/an101223.pdf, abgerufen am 11.05.2018.

21 Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting.

22 Steffens, Hacker-Jagd im Cyberspace – Grundlagen und Grenzen der Suche nach den Tätern in: c't 14/2017, Seite 122.

23 Vgl. BSI-Standard 200-2, Seite 12.

24 BSI, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, abgerufen am 30.07.2018.

25 Geiß, Völkerrecht im „Cyberwar", http://www.ipg-journal.de/schwerpunkt-des-monats/neue-high-tech-kriege/artikel/detail/voelkerrecht-im-cyberwar-859/, abgerufen am 11.05.2018.

Wegen der überragenden Bedeutung der Cybersicherheit für den Finanzsektor hat die G7 Cyber Expert Group einen Bericht über die grundlegenden Elemente für die wirksame Bewertung der Cybersicherheit im Sektor vorgelegt, der am 12. Oktober 2017 von den Finanzministern und den Zentralbankpräsidenten der G7 angenommen wurde.[26] Derzeit prüft die BaFin, inwieweit die BAIT angepasst beziehungsweise ergänzt werden müssen, um den Vorgaben des G7-Berichts gerecht zu werden, etwa um Anforderungen an das Notfallmanagement[27] und entsprechende Übungen.

26 Siehe Bundesministerium der Finanzen: https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2017-10-27-Cyber-Security-download.pdf?__blob=publicationFile&v=2, abgerufen am 11.05.2018.

27 Lawrence, Cybersimulation: Der Teufel, den man kennt, in: Herbert Frommes Versicherungsmonitor, https://versicherungsmonitor.de/2018/05/03/cybersimulation-der-teufel-den-man-kennt/, abgerufen am 11.05.2018.

4 EBA-Regulierung mit IT-Bezug

Weil Digitalisierung kein nationales Thema ist, ist es essenziell, europaweit ein gemeinsames Verständnis und einheitliche regulatorische Anforderungen dazu zu entwickeln. Die Europäische Bankenaufsichtsbehörde EBA (European Banking Authority), in der auf verschiedenen Ebenen auch die BaFin vertreten ist, ist federführend für die Harmonisierung der Aufsichtspraxis in der Europäischen Union (EU) zuständig.

Am 7. Juli 2014 hat die EBA Leitlinien zum aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process – SREP) veröffentlicht.[28] Der SREP schließt die Beurteilung der Schlüsselindikatoren, des Geschäftsmodells, der *Governance* und der Kapital- und Liquiditätsrisiken ein. Die EBA hat in ihren SREP-Leitlinien erstmals den Begriff „IT-Risiko" definiert (siehe Infokasten „Definition IT-Risiko").

Definition

IT-Risiko

Das Informations- und Kommunikationstechnologie-Risiko (IKT-Risiko) ist laut SREP-Leitlinien der EBA [GL/2014/13] „[…] das bestehende oder künftige Risiko von Verlusten aufgrund der Unzweckmäßigkeit oder des Versagens der Hard- und Software technischer Infrastrukturen, welche die Verfügbarkeit, Integrität, Zugänglichkeit und Sicherheit dieser Infrastrukturen oder von Daten beeinträchtigen können[29]."

Um das IT-Risiko innerhalb des SREPs noch genauer validieren und bewerten zu können, hat die EBA am 11. Mai 2017 konkretisierende Leitlinien[30] erlassen. Ergänzend zum allgemeinen SREP hat sie darin ein IT-SREP-Verfahren für bedeutende Institute (*Significant Institutions* – SIs) und eines für weniger bedeutende Institute (*Less Significant Institutions* – LSIs) entwickelt.

Gemäß Tz. 5 zielen die IT-SREP-Leitlinien vom Mai 2017 darauf ab, die Konvergenz der Aufsichtspraktiken bei der Bewertung des IT-Risikos im Rahmen des SREPs sicherzustellen. Die Leitlinien enthalten hierfür Bewertungskriterien, welche die zuständigen Behörden bei der aufsichtlichen Bewertung der IT-Governance und IT-Strategie der Institute und bei der aufsichtlichen Bewertung von deren IT-Risikopositionen und -kontrollen anwenden sollten.

Außerdem hat die Aufsicht zu bewerten, ob der allgemeine Governance-Rahmen und der interne Kontrollrahmen des Instituts die IT-Systeme und die damit verbundenen Risiken ordnungsgemäß abdecken und ob das Leitungsgremium diese Aspekte angemessen angeht und verwaltet, da die IT für das ordnungsgemäße Funktionieren eines Instituts von zentraler Bedeutung ist. Insbesondere hat die Aufsicht zu beurteilen,

- ob das Institut über eine angemessene IT-Strategie verfügt, die hinreichend geregelt ist und mit dessen Geschäftsstrategie in Einklang steht,
- ob die internen Governance-Regelungen des Instituts in Bezug auf die IT-Systeme des Instituts angemessen sind
- und ob der Risikomanagementrahmen und der interne Kontrollrahmen des Instituts dessen IT-Systeme angemessen sichern.

Auch sollen die Aufseher auf der Basis des Titels 5 der EBA-SREP-Leitlinien vom Juli 2014 bewerten, ob das Institut über eine angemessene und transparente Unternehmensstruktur verfügt, die zweckdienlich ist, und ob es entsprechende Governance-Regeln umgesetzt hat. Mit Blick auf die IT-Systeme und im Einklang mit den EBA-Leitlinien zur internen *Governance*[31] soll sie prüfen, ob das Institut über eine solide und transparente Organisationsstruktur verfügt, in der die Verantwortlichkeiten in Bezug auf die IT klar definiert sind. Das gilt auch für das Leitungsorgan und seine

28 EBA-Leitlinien EBA/GL/2014/13.
29 EBA-Leitlinien EBA/GL/2014/13, a.a.O., Seite 74.
30 EBA-Leitlinien EBA/GL/2017/05. Das Kürzel „IKT" steht für Informations- und Kommunikationstechnik.
31 EBA-Leitlinien EBA/GL/44.

Ausschüsse. Zu prüfen ist auch, dass wichtige, für die IT verantwortliche Personen wie etwa der *Chief Information Officer* (CIO) und der *Chief Operating Officer* (COO) über einen ausreichenden indirekten oder direkten Zugang zum Aufsichtsorgan verfügen. So soll sichergestellt werden, dass auch das Aufsichtsorgan die mit der IT verbundenen Risiken kennt und sich mit ihnen befasst.

Da die Bedeutung von IT-Auslagerungen für den Geschäftserfolg weiter zunimmt, aber auch mit Blick auf die damit verbundenen Sicherheitsrisiken fordern die Leitlinien, dass die Aufsichtsbehörden bewerten, ob die IT-Auslagerungspolitik und -strategie des Instituts die Auswirkungen der IT-Auslagerung auf das Geschäft und das Geschäftsmodell des Instituts berücksichtigen.

5 Aufsichtliche Anforderungen an die IT der Institute mit KWG-Lizenz

Auch in Deutschland ist die IT-Aufsicht mehr und mehr in den Fokus aufsichtlichen Handelns gerückt. Schon 2012 hat die BaFin das Referat „IT-Infrastrukturen bei Banken" eingerichtet. Zum Jahresbeginn 2018 wurde die Gruppe „IT-Aufsicht / Zahlungsverkehr / Cybersicherheit" gegründet, in der dieses Referat aufgegangen ist. Die Gruppe ist unter anderem für Grundsatzfragen zur Cybersicherheit, der Aufsicht über Zahlungs- und E-Geldinstitute, Prüfungen mit IT-Bezug und Grundsatzfragen zur IT-Aufsicht zuständig. Die IT-Aufsicht erfolgt seitdem geschäftsbereichsübergreifend und soll nachfolgend exemplarisch am Beispiel des Kreditwesengesetzes (KWG) dargestellt werden:

Die Generalnorm für die Aufsicht über Institute in § 6 Abs. 2 KWG lautet: „Die Bundesanstalt hat Mißständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können."

Die BaFin interpretiert dies so, dass die „den Instituten anvertrauten Vermögenswerte" heute in der Regel Daten sind, die in IT-Systemen verarbeitet und gespeichert werden. Eine Beeinträchtigung der ordnungsmäßigen Durchführung der Bankgeschäfte oder Finanzdienstleistungen ist somit immer mindestens dann anzunehmen, wenn

- die Verfügbarkeit der IT-Systeme unzureichend ist, das heißt, wenn also die IT-Systeme nicht bestimmungsgemäß betriebsbereit sind und die Verarbeitung der Daten nicht korrekt abläuft,
- die Datenintegrität nicht vollständig gewährleistet werden kann, wenn also die Korrektheit der Daten (Datenintegrität) und / oder die Korrektheit der Funktionsweise des IT-Systems (Systemintegrität) nicht sichergestellt ist beziehungsweise
- die Vertraulichkeit nicht sichergestellt werden kann, sprich: wenn es möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.

Konkretisiert werden die allgemeinen Aufgaben der Bankenaufsicht nach § 6 KWG durch § 25a Abs. 1 KWG (siehe Infokasten).

Was die BaFin mit Blick auf die IT konkret unter einer ordnungsgemäßen Geschäftsorganisation versteht, hat sie insbesondere in ihren BAIT niedergelegt.

Info

§ 25a Abs. 1 KWG

Dieser Paragraf gibt vor, dass „ ein Institut […] über eine ordnungsgemäße Geschäftsorganisation verfügen [muss], die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. Die Geschäftsleiter sind für die ordnungsgemäße Geschäftsorganisation des Instituts verantwortlich; sie haben die erforderlichen Maßnahmen für die Ausarbeitung der entsprechenden institutsinternen Vorgaben zu ergreifen, sofern nicht das Verwaltungs- oder Aufsichtsorgan entscheidet.

Eine ordnungsgemäße Geschäftsorganisation muss insbesondere ein angemessenes und wirksames Risikomanagement umfassen, […]; das Risikomanagement umfasst insbesondere […]

4. eine angemessene personelle und technischorganisatorische Ausstattung des Instituts;

5. die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme […] ."

6 Interpretation der Aufsichtsnormen durch die BAIT

Allgemeine Hinweise
Die BAIT interpretieren – ebenso wie die Ende Oktober 2017 überarbeiteten MaRisk[32] – die gesetzlichen Anforderungen des § 25a Abs. 1 Satz 3 Nrn. 4 und 5 KWG. Da die Institute immer mehr IT-Dienstleistungen von Dritten in Anspruch nehmen, weil sie zum Beispiel IT-Dienstleistungen auslagern, beziehen die BAIT auch den § 25b KWG in diese Interpretation ein. Dort wird unter anderem der Umgang mit der Auslagerung von Aktivitäten und Prozessen geregelt. Durch Verweise auf konkrete Textziffern in den MaRisk wird der Bezug der BAIT zu den allgemeinen bankaufsichtlichen Anforderungen an das Risikomanagement sichergestellt.

Die BAIT in der vorliegenden ersten Fassung adressieren insbesondere Themen, bei denen die Aufsicht in den vergangenen Jahren bei Prüfungen wesentliche Mängel identifiziert hat. Dazu gehören zum Beispiel die IT-Strategie und die IT-Governance, die Informationssicherheit, das Berechtigungsmanagement und die Anwendungsentwicklung sowie der Bezug von IT-Dienstleistungen von Dritten im Sinne von IT-Auslagerungen beziehungsweise der Fremdbezug von IT-Dienstleistungen.

Die BAIT sollen insbesondere dem Management der Institute und – mittelbar über die Auslagerungsverträge – auch dem IT-Dienstleister dabei helfen, auch mit Blick auf die IT-Aufbau- und -Ablauforganisation und bei der Nutzung der IT-Systeme eine ordnungsgemäße Geschäftsorganisation sicherzustellen. Die als Prinzipien formulierten Anforderungen der BAIT sind jedoch nicht als vollständiger Anforderungskatalog anzusehen. Insoweit bleiben die Institute und ihre IT-Dienstleister gemäß AT 7.2 MaRisk in der Pflicht, bei der Umsetzung der BAIT-Anforderungen auf gängige Standards abzustellen und diese wirksam zu implementieren.

Darüber hinaus ist es ein Wesensmerkmal der BAIT, dass der Grundsatz der doppelten Proportionalität uneingeschränkt gilt.

IT-Risikobewusstsein schärfen
Ein zentrales Ziel der BAIT ist es, das IT-Risikobewusstsein in den Instituten und insbesondere auf den Führungsebenen zu schärfen. Der hier einschlägige Begriff „IT-Risiko" wurde bereits oben[33] definiert. Das Erfordernis, Risikotransparenz zu schaffen und sich mit dem IT-Risiko auf allen Ebenen des Instituts auseinanderzusetzen, zieht sich durch alle acht Themenmodule der BAIT und ist integraler Bestandteil der Anforderungen in den einzelnen Textziffern.

IT-Strategie – II.1. BAIT
In Bezug auf die IT-Strategie steht die Anforderung im Vordergrund, dass sich die Geschäftsleitung regelmäßig mit den strategischen Implikationen der verschiedenen Aspekte der IT für die Geschäftsstrategie auseinandersetzt. Hierzu gehören neben der Aufbau- und Ablauforganisation der IT im Institut zum Beispiel auch der Umgang mit der individuellen Datenverarbeitung (IDV) in den Fachbereichen, strategische Aussagen zum externen Bezug von IT-Dienstleistungen (Auslagerung von IT-Dienstleistungen beziehungsweise Fremdbezug von IT) und grundlegende Anforderungen an das Notfallmanagement.

Die Geschäftsleitung hat die IT-Strategie in einem zyklischen Prozess zu erarbeiten und nach Erörterung mit dem Aufsichtsorgan zu beschließen und institutsintern zu veröffentlichen. Durch die darin formulierten Maßnahmen zur Erreichung der Strategieziele wird auch Klarheit darüber geschaffen, welche Bedeutung die IT für die Durchführung der Bankgeschäfte hat. Des Weiteren erwartet die Aufsicht insbesondere auch strategische Aussagen zum IT-Risikobewusstsein, aber auch Hinweise zur Einhaltung der Anforderungen an die Informationssicherheit im Institut und gegenüber Dritten.

Governance – II.2. BAIT
Die IT-Governance ist die Struktur zur Steuerung und Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der dazugehörigen IT-Prozesse auf Basis der IT-Strategie. Die Geschäftsleitung ist dafür verantwortlich, dass die Regelungen zur

32 Rundschreiben 09/2017 (BA) – Mindestanforderungen an das Risikomanagement (MaRisk).

33 Siehe Seite 75.

IT-Governance institutsintern und gegenüber Dritten wirksam umgesetzt werden. Sie hat auch dafür Sorge zu tragen, dass insbesondere das Informationsrisiko- und das Informationssicherheitsmanagement, der IT-Betrieb und die Anwendungsentwicklung angemessen mit Personal ausgestattet sind. Dies ist aus Sicht der BaFin vor allem deshalb wichtig, weil auf diese Weise das Risiko einer qualitativen oder quantitativen Unterausstattung dieser Bereiche frühzeitig erkannt und möglichst umgehend behoben werden kann.

Informationsrisikomanagement – II.3. BAIT
Das Institut hat im Rahmen des Managements der Informationsrisiken den Schutzbedarf der relevanten Daten beziehungsweise Informationen zu ermitteln. Auf dieser Grundlage sind Soll-Maßnahmen festzulegen und diese mit den wirksam umgesetzten Ist-Maßnahmen zu vergleichen. Die daraus resultierende Transparenz der Risikosituation, die Ableitung risikomindernder Maßnahmen und die Überwachung von deren wirksamer Umsetzung sowie die Kenntnis des ermittelten Restrisikos seitens der Geschäftsleitung sind zentrale Anforderungen zur Schärfung des IT-Risikobewusstseins im Institut und gegenüber IT-Dienstleistern.

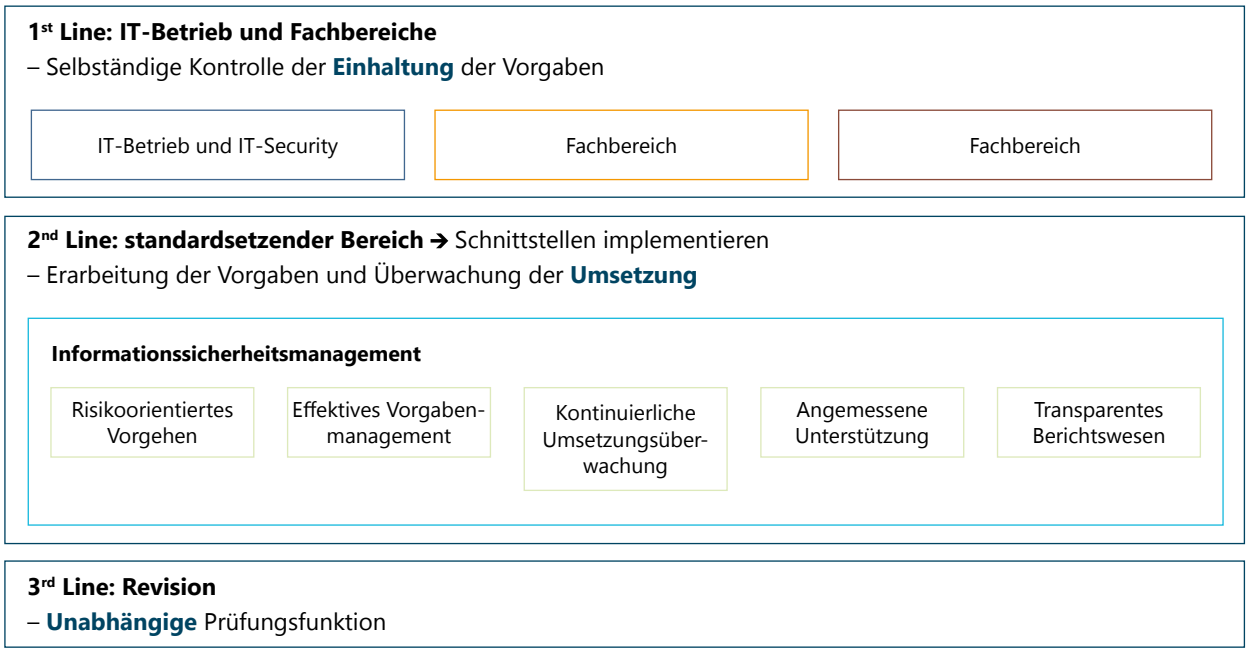
Damit neben den IT-Risiken auch die einschlägigen Risiken mit IT-Bezug adäquat gesteuert werden können, erwartet die Aufsicht von den Instituten, dass sie einen aktuellen Überblick über die Bestandteile des festgelegten Informationsverbunds[34] sowie deren Abhängigkeiten und Schnittstellen haben. Das Institut sollte sich hierbei insbesondere an den betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation orientieren. Um ihrer Managementverantwortung gerecht werden zu können, ist die Geschäftsleitung regelmäßig, mindestens jedoch vierteljährlich, vor allem über die Ergebnisse der Risikoanalyse und Veränderungen der IT-Risikosituation zu unterrichten.

Informationssicherheitsmanagement – II.4. BAIT
Das Informationssicherheitsmanagement macht Vorgaben zur Informationssicherheit, definiert entsprechende Prozesse und steuert deren Umsetzung. Die Aufsicht betrachtet die Informationssicherheit als Teil der 2. Verteidigungslinie im Sinne des Three-Lines-of-Defense-Modells (siehe Grafik 1 „Three-Lines-of-Defence-Modell", Seite 80), die die operative 1. Linie überwacht, aber auch unterstützt.

Die Geschäftsleitung ist dafür verantwortlich, unter Berücksichtigung der festgestellten Risikosituation eine Informationssicherheitsleitlinie zu beschließen und hausintern zu veröffentlichen. Die im Rahmen des

34 Zu einem Informationsverbund gehören beispielsweise geschäftsrelevante Informationen, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen.

Grafik 1: Three-Lines-of-Defence-Modell



© Quelle: Eigene Darstellung – in Anlehnung an Three-Lines-of-Defence-Modell aus dem Occasional Paper Nr. 11 der BIS, 2015, Bank for International Settlements (BIS).

Informationsrisikomanagements definierten Schutzbedarfe sind durch Informationssicherheitsrichtlinien zu konkretisieren.

Der Informationssicherheitsbeauftragte (ISB)[35] oder – bei größeren Instituten – das Informationssicherheitsmanagement-System (ISMS)[36] sind aus Sicht der Aufsicht die maßgeblichen Instanzen für die Umsetzung, Einhaltung und Überwachung der unternehmensinternen Vorgaben für die Informationssicherheit innerhalb des Instituts und gegenüber Dritten auf der Basis der aufsichtlichen Anforderungen unter Einbeziehung der einschlägigen Standards. Deshalb ist die Funktion des Informationssicherheitsbeauftragten organisatorisch und prozessual unabhängig auszugestalten, so dass die Bewertung der Informationssicherheit und – soweit notwendig – die Bearbeitung von Informationssicherheitsvorfällen frei von Interessenkonflikten erfolgen können.

Der ISB hat der Geschäftsleitung regelmäßig (mindestens vierteljährlich) und anlassbezogen zu berichten.

Vor allem mit Blick auf das zunehmende Cyberrisiko erwartet die Aufsicht, dass diese Funktion quantitativ und qualitativ angemessen mit personellen und finanziellen Ressourcen ausgestattet ist – so, wie es sich aus § 25a KWG i.V.m. AT 7.1 MaRisk und den einschlägigen Standards (BSI-Standard 200-2, Seite 40 ff; ISO/IEC 27001: 2013, 4.4) ableiten lässt. Selbstverständlich beachtet sie auch dabei das Proportionalitätsprinzip und hat spezielle Erleichterungen insbesondere für kleine Institute formuliert.

Benutzerberechtigungsmanagement – II.5. BAIT

Berechtigungen zum Zugriff auf genau definierte Teile von IT-Systemen sind notwendig, damit bestimmte Aufgaben erfüllt werden können. Sie sind aber auch ein zentraler Baustein bei der Schaffung von IT-Sicherheit. Im Rahmen des Benutzerberechtigungsmanagements ist deshalb das Berechtigungskonzept schriftlich festzulegen. Bei der Erarbeitung des Konzepts sind die Fachbereiche einzubeziehen. Beim Berechtigungskonzept ist das

35 Siehe Bundesamt für Sicherheit in der Informationstechnik (BSI)-Standard 200-2, Seite 40 ff.
36 Siehe ISO/IEC 27001: 2013, 4.4.

Need-to-know-Prinzip anzuwenden, das besagt, dass nur die Berechtigungen zu genehmigen und einzurichten sind, die für die Erfüllung einer konkreten Aufgabe benötigt werden. Das gilt auch für den Rezertifizierungsprozess, in dem geprüft werden muss, ob eingeräumte Berechtigungen weiter notwendig sind. Sollte dies nicht mehr der Fall sein, müssen die Berechtigungen wirksam entzogen werden.[37]

IT-Projekte und Anwendungsentwicklung – II.6. BAIT

Bei der Steuerung und Überwachung von IT-Projekten sind insbesondere die Risiken im Hinblick auf die Dauer, den Ressourcenverbrauch und die Qualität zu berücksichtigen. Die Geschäftsleitung hat dafür Sorge zu tragen, dass eine Gesamtübersicht der IT-Projektrisiken und der Risiken erstellt wird, die sich aus den Abhängigkeiten verschiedener Projekte untereinander ergeben.

Bereits bei der Entwicklung von Anwendungen sind Vorkehrungen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der in diesem Programm zu verarbeitenden Daten sicherstellen. Diese Vorgaben dienen insbesondere dazu, das Risiko zu reduzieren, dass die Anwendung versehentlich geändert oder absichtlich manipuliert wird. An dieser Stelle sei auch noch einmal auf die Ausführungen zur Einbindung der einschlägigen Sicherheitsmaßnahmen im Sinne des *Security by Design* verwiesen.[38]

Darüber hinaus ist es aus Sicht der BaFin stets sinnvoll, Anwendungen der individuellen Datenverarbeitung (IDV-Anwendungen), die die Fachbereiche entwickeln beziehungsweise betreiben, in Risikoklassen einzuteilen und diese Einteilung regelmäßig zu evaluieren. Die Aufsicht erwartet auch, dass jedes Institut alle IDV-Anwendungen in einem zentralen Register führt, die insbesondere für bankgeschäftliche Prozesse, für die Risikosteuerung und -überwachung oder für die Rechnungslegung Bedeutung haben.

IT-Betrieb – II. 7. BAIT

Der IT-Betrieb hat in erster Linie die Anforderungen zu erfüllen, die sich aus der Umsetzung der Geschäftsstrategie und aus den IT-unterstützten Geschäftsprozessen ergeben, und hierbei auch das Portfolio der IT-Systeme angemessen zu steuern. Des Weiteren soll er technische Innovationen nach Maßgabe der Fachbereiche aufgreifen und – gegebenenfalls in Projektform – in die IT-Produktion überführen.

Die entsprechenden Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risikogehalt auszugestalten und umzusetzen (Proportionalität). Dies gilt ebenso für Neu- beziehungsweise Ersatzbeschaffungen von IT-Systemen sowie für sicherheitsrelevante Nachbesserungen (Sicherheitspatches). Im Rahmen des Produktlebenszyklus-Managements sind hierbei auch die Risiken zu überwachen, die aus veralteten IT-Systemen resultieren. Dies ist jedoch nur möglich, wenn alle Komponenten der IT-Systeme inklusive der Bestandsangaben und die gegenseitigen Abhängigkeiten der verwalteten Objekte angemessen geführt werden. Hierfür sollten mittlere und große Institute grundsätzlich eine *Configuration Management Database* (CMDB) nutzen, kleine zumindest ein Inventarverzeichnis. Die erfassten Informationen sind regelmäßig und anlassbezogen zu aktualisieren.

Für den Fall, dass es ungeplante Abweichungen vom Regelbetrieb gibt, sind vorab geeignete Kriterien für die Information der Geschäftsleitung über mögliche Ursachen dieser Störung, über die zu ergreifenden Notfallmaßnahmen zur Aufrechterhaltung beziehungsweise Wiederherstellung des Geschäftsbetriebs und über die Beseitigung der Mängel schriftlich festzulegen. Im Rahmen des Notfallmanagements[39] gemäß AT 7.3 MaRisk sind regelmäßig jeweils zu dokumentierende Notfallübungen im Institut und gegebenenfalls gemeinsam mit bedeutenden IT-Dienstleistern durchzuführen und zu evaluieren und festgestellte Schwächen und Mängel zu beseitigen.

37 Siehe BSI, IT-Grundschutz: M 2.8 Vergabe von Zugriffsrechten.
38 Siehe Seite 72.
39 Siehe BSI-Grundschutz 100-4 oder ISO 22301:2012.

Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen – II. 8. BAIT

Nimmt ein Institut IT-Dienstleistungen in Anspruch, gilt grundsätzlich dasselbe wie bei der Inanspruchnahme von Dienstleistungen allgemein: Das Institut hat zu prüfen, ob es sich um eine Auslagerung im Sinne des § 25b KWG handelt. Ist dies der Fall, hat sie die Anforderungen des § 25b KWG und AT 9 der MaRisk zu erfüllen, und das Institut muss vorab eine Risikoanalyse durchführen. Die Risiken aus dem sonstigen Fremdbezug von IT-Dienstleistungen, deren Definition ebenfalls in AT 9 MaRisk zu finden ist, sind ebenfalls vorab zu bewerten. Nur so kann das Institut seine vollständige Risikosituation ermitteln und Konzentrationsrisiken bei den extern bezogenen IT-Dienstleistungen erkennen. Des Weiteren erwartet die Aufsicht, dass die aus der jeweiligen Risikoanalyse abgeleiteten Maßnahmen in die Gestaltung der einzelnen Verträge mit dritten Dienstleistungserbringern einfließen. Bei wesentlichen Auslagerungen von IT-Dienstleistungen sind die Vorgaben des AT 9 Tz. 7 MaRisk einzuhalten; dies gilt selbstverständlich auch bei *Cloud Computing*.[40]

Umsetzung der BAIT

Die BAIT sind mit ihrer Veröffentlichung am 6. November 2017 in Kraft getreten. Eine Umsetzungsfrist oder Übergangsfristen hat die BaFin nicht vorgesehen, denn in den BAIT werden keine neuen Anforderungen an die Institute und ihre Dienstleister gestellt. Bei der Jahresabschlussprüfung 2018 werden die einschlägigen Vorgaben der Prüfungsberichtsverordnung (PrüfbV) unter Einbeziehung der BAIT erstmals Berücksichtigung finden. Prüfungen nach § 44 KWG mit IT-Fokus orientieren sich seit Anfang 2018 ebenfalls an den BAIT.

Mögliche Anpassungen der BAIT

Die modulare Ausgestaltung der BAIT eröffnet der Aufsicht die notwendige Flexibilität für künftige Anpassungen oder Ergänzungen. Die BaFin hat bereits mehrfach angekündigt, dass das Thema „IT-Notfallmanagement inklusive Test- und Wiederherstellungsverfahren" in die BAIT integriert werden soll.

Sie prüft derzeit auch, ob die BAIT an die „G7 – Fundamental Elements of Cybersecurity"[41] und die „Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)"[42] angepasst werden müssen.

Des Weiteren erwägt die BaFin – in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) – ein spezielles Modul zu Kritischen Infrastrukturen (KRITIS), das die BAIT ergänzen soll. Dieses spezielle Modul soll ausschließlich für diejenigen Banken und IT-Dienstleister gelten, die KRITIS-Betreiber im Sektor Finanz- und Versicherungswesen im Sinne des § 2 Abs. 10 BSI-Gesetz sind. Es soll die notwendigen Anforderungen formulieren, die diese KRITIS-Betreiber erfüllen müssen, um den einschlägigen Vorgaben des § 8a Abs. 3 BSI-Gesetz nachzukommen.

40 Vgl. BaFinJournal April 2018, Seite 29 ff.

41 Vgl. hierzu Abschnitt 3.

42 EBA-Leitlinien EBA/GL/2017/17; Payment Services Directive 2.

7 Digitalisierung der Versicherungswirtschaft

Die Digitalisierung als eines der zentralen strategischen Themen in der Versicherungswirtschaft
Neben unternehmensinterner Prozessoptimierung und Effizienzsteigerung geht es bei der Digitalisierung im Versicherungssektor vor allem um die Verbesserung des Kontakts zum Kunden.[43] Versicherungsunternehmen haben in den vergangenen Jahren bereits viele ihrer Geschäftsprozesse – intern und im Vertrieb – gestrafft und automatisiert. Insbesondere durch Automatisierung manueller Prozessschritte hin zu einer möglichst volldigitalen Abwicklung von Antrags-, Vertrags- und Schadenprozessen lässt sich die interne Automatisierungsquote deutlich steigern. Über Skaleneffekte lassen sich zudem Kosten senken. So weisen bereits viele standardisierbare Prozesse, wie etwa Bestandsverwaltung und Schadenmanagement, einen hohen Automatisierungsgrad auf.[44]

Ein weiterer Fokus liegt bei der Digitalisierung in der Versicherungswirtschaft auf der Ausgestaltung der Kundenschnittstellen. Die digitale Transformation der Versicherungsunternehmen kann nur gelingen, wenn Kundenbindung und Kundenzufriedenheit mindestens gehalten und, besser noch, erheblich gesteigert werden können. Hierzu ist es essenziell, dem Kunden einen messbaren Mehrwert zu verschaffen – im besten Fall ein aus seiner Sicht optimales Kundenerlebnis.[45]

Neue Herausforderungen im Versicherungsvertrieb – die Cyberversicherung
Verschiedene Untersuchungen zeigen, dass Cybergefahren sowohl international[46] als auch auf der Risikoagenda deutscher Unternehmen in letzter Zeit immer weiter nach oben gerückt sind. Im aktuellen Allianz Risk Barometer der Allianz Global Corporate & Speciality SE (AGCS) wird dargestellt, dass Cyberangriffe inzwischen auf Position zwei der am meisten gefürchteten Unternehmensrisiken angekommen seien.[47]

Auch die deutsche Versicherungswirtschaft hat auf diese Situation reagiert und ein Produkt Cyberversicherung

43 Versicherungsforen Leipzig, Digitalisierung der Customer Journey bei Versicherungen in der DACH-Region, https://www.liferay.com/documents/10182/171894549/Digitalisierung%20der%20Customer%20Journey%20bei%20Versicherungen%20in%20der%20DACH-Region, abgerufen am 11.05.2018.

44 Bain & Company, Digitalisierung der Versicherungswirtschaft: Die 18-Milliarden-Chance, Seite 21, http://www.bain.de/Images/161202_Bain-Google-Studie_Digitalisierung_der_Versicherungswirtschaft.pdf, abgerufen am 11.05.2018.

45 IT Finanzmagazin, Whitepaper der Versicherungsforen Leipzig & NICE: Kunden und Digitalisierung treiben die Assekuranz, https://www.it-finanzmagazin.de/whitepaper-der-versicherungsforen-leipzig-nice-kunden-und-digitalisierung-treiben-die-assekuranz-31078, abgerufen am 11.05.2018.

46 datensicherheit.de: Cyber-Sicherheitsvorfälle: Neuer Kaspersky-Bericht über Folgekosten liegt vor, https://www.datensicherheit.de/aktuelles/cyber-sicherheitsvorfaelle-neuer-kaspersky-bericht-ueber-folgekosten-liegt-vor-25899, abgerufen am 11.05.2018.

47 Allianz Risk Barometer, https://www.allianzdeutschland.de/allianz-risk-barometer-2018/id_79713564/index, abgerufen am 11.05.2018.

in verschiedenen Ausprägungen entwickelt.[48] Der Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) hat hierzu – als unverbindlich deklarierte – allgemeine Versicherungsbedingungen (AVB Cyber) veröffentlicht, die extrem weitgehende Anforderungen an die Antragsteller stellen, die dieses Risiko versichern wollen.[49]

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Es wird nicht überraschen, dass die Aufsicht auch von der Branche, die Cyberrisiken versichern kann, erwartet, dass sie die grundlegenden Anforderungen einhält und wirksam umgesetzt hat, die an die IT-Governance, das IT-Risiko- und Informationssicherheitsmanagement, die Anwendungsentwicklung und den Betrieb von IT-Systemen gestellt werden. Hierzu hat die BaFin Mitte März 2018 den Entwurf des Rundschreibens „Versicherungsaufsichtliche Anforderungen an die IT (VAIT)" zur Konsultation gestellt.[50] Am 2. Juli 2018 hat sie die VAIT publiziert.

Die VAIT sollen – vergleichbar mit den BAIT für den Bankensektor – der zentrale Baustein der IT-Aufsicht über all die Versicherungsunternehmen und Pensionsfonds (Unternehmen) sein, die in den Textziffern 2 und 3 der Vorbemerkung zu den VAIT benannt sind.[51]

Das Rundschreiben enthält Hinweise zur Auslegung der Vorschriften des Versicherungsaufsichtsgesetzes (VAG) zur Geschäftsorganisation, soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen (siehe Infokasten „Interpretation des VAG durch die VAIT").

Interpretation des VAG durch die VAIT

Die VAIT interpretieren zum Beispiel die §§ 23, 26 und 32 Versicherungsaufsichtsgesetz (VAG).

Die VAIT konkretisieren also, was die Aufsicht unter einer angemessenen Ausgestaltung der IT-Systeme (Hard- und Software-Komponenten) und der dazugehörigen IT-Prozesse versteht, und zwar unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit. Da inzwischen viele Unternehmen IT-Dienstleistungen von Dritten in Form von Ausgliederungen oder sonstigen Dienstleistungsbeziehungen beziehen, sind auch dazu Anforderungen in den VAIT formuliert.

Die VAIT sollen transparent machen, was die Aufsicht von den Unternehmen und ihren IT-Dienstleistern verlangt. Sie sollen ihnen auf diese Weise helfen, auch mit Blick auf die IT eine ordnungsgemäße und wirksame Geschäftsorganisation sicherzustellen. Da die Anforderungen jedoch keinen vollständigen Vorgabenkatalog darstellen und hinsichtlich Regelungstiefe und -umfang nicht abschließend sind, bleibt jedes Unternehmen folglich auch insbesondere jenseits der Konkretisierungen durch die VAIT verpflichtet, grundsätzlich auf gängige IT-Standards abzustellen und den Stand der Technik zu berücksichtigen.

Bei der Umsetzung der Anforderungen der VAIT an die Geschäftsorganisation und somit auch der Ausgestaltung der Strukturen, IT-Systeme oder Prozesse der Unternehmen spielt auch das Proportionalitätsprinzip eine erhebliche Rolle. Die Anforderungen sind also auf eine Art und Weise zu erfüllen, die der Wesensart, dem Umfang und der Komplexität der Risiken gerecht wird, die mit der Tätigkeit des Unternehmens einhergehen.

Auch bei den VAIT ziehen sich das Erfordernis, Risikotransparenz zu schaffen, und die Notwendigkeit, sich mit dem IT-Risiko auf allen Ebenen des Unternehmens und seiner IT-Dienstleister auseinanderzusetzen, durch alle Themenbereiche.

48 VersicherungsJournal.de, Signal Iduna bringt Cyber-Schutzschild auf den Markt, https://www.versicherungsjournal.de/versicherungen-und-finanzen/signal-iduna-bringt-cyber-schutzschild-auf-den-markt-131904.php, abgerufen am 11.05.2018.

49 GDV, AVB Cyber, hier: A 1-16 (insbesondere A 1-16.2 a), https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0c-c207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf, abgerufen am 11.05.2018.

50 www.bafin.de/dok/10622504.

51 Vgl. BaFinJournal April 2018, Seite 24 ff.

8 Zusammenfassung

Die Digitalisierung hat bereits zu erheblichen und teilweise einschneidenden Veränderungen in der Finanz- und Versicherungswirtschaft geführt und wird dies weiterhin tun. Viele Kunden wollen überall und zu jeder Zeit mit Banken und Versicherern interagieren können. Entsprechend hoch sind ihre Erwartungen an die Unternehmen, was die Sicherheit und Integrität ihrer Daten angeht. Dies führt zu einem intensiven Wettstreit der etablierten Anbieter mit neuen innovativen Wettbewerbern.

Banken und Versicherungen verfügen über zwei in einer digitalen Welt notwendige Rohstoffe: Vertrauen und Daten. Der derzeit auch am Finanzmarkt zu beobachtende zunehmende Einsatz von *Big Data* (BD) und künstlicher Intelligenz (*Artificial Intelligence* – AI) stellt sowohl die Industrie als auch die Regulierung, insbesondere aber auch die Kunden vor gewaltige Herausforderungen. Bei allem notwendigen Veränderungsdruck wären die Unternehmen allein aus wirtschaftlichem Kalkül gut beraten, genau zu überlegen, inwieweit sie die neuen technischen Möglichkeiten tatsächlich ausreizen wollen, etwa bei der Monetarisierung persönlicher Daten mithilfe von BDAI-Anwendungen. Ansonsten laufen sie in bestimmten Fällen Gefahr, dass Reputationsschäden den Nutzen überwiegen könnten.

Die Aufgabe der BaFin ist es in erster Linie, ein funktionsfähiges, stabiles und integres Finanzsystem zu gewährleisten. Sie wird ihrer Aufgabe gerecht, indem sie beispielsweise aufsichtliche Anforderungen an die Geschäftsorganisation der am Finanzmarkt tätigen erlaubnispflichtigen Unternehmen stellt. Selbstverständlich geht der digitale Wandel auch an Aufsichtsbehörden nicht spurlos vorbei. Regelmäßig muss evaluiert werden, welche neuen Anforderungen rechtlicher und technischer Art die Innovationswelle, die Gesellschaft und Wirtschaft gegenwärtig erleben, an Regulierung und Aufsicht stellt. Abschließende Antworten darauf kann gegenwärtig niemand geben. Umso wichtiger sind eine ständige Auseinandersetzung mit solchen Fragen und der regelmäßige Austausch zwischen Behörden, Unternehmen und Wissenschaft.

Es wird eine gesamtgesellschaftliche Aufgabe sein müssen, die Balance zwischen der Renditeerwartung der Unternehmen, der notwendigen Überwachung der Einhaltung der Anforderungen an die *Governance* und die Cybersicherheit durch die Aufsicht sowie der informationellen Selbstbestimmung der Verbraucher zu schaffen und auch langfristig sicherzustellen.

Impressum

Herausgeber
Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108 | 53117 Bonn
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main
www.bafin.de

Redaktion und Layout
BaFin, Öffentlichkeitsarbeit und Reden
Redaktion: Ursula Mayer-Wanders (Leitung)
Tel.: +49 (0)228 4108-2978
Jens Valentin
Tel.: +49 (0)228 4108-2363

Layout: Susanne Geminn
Tel.: +49 (0)228 4108-3091

E-Mail: perspektiven@bafin.de

Designkonzept
werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt
www.werksfarbe.com

Bonn und Frankfurt am Main | 1. August 2018
ISSN 2625-5952

Bezug
Die Schriftenreihe BaFinPerspektiven erscheint zweimal im Jahr auf der Internetseite der BaFin jeweils in deutscher und englischer Sprache. Die englische Ausgabe erscheint unter dem Titel „BaFinPerspectives“. Mit dem Abonnement des Newsletters der BaFin werden Sie über das Erscheinen einer neuen Ausgabe per E-Mail informiert. Den BaFin-Newsletter finden Sie unter: www.bafin.de » Newsletter.

Druck
Druckerei Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal