Zahlungsverkehr

Susan Emmenegger (Hrsg.)

Institut für Bankrecht, Universität Bern

SBT 2018 – Schweizerische Bankrechtstagung 2018

Zahlungsverkehr

herausgegeben von Susan Emmenegger

mit Beiträgen von
Marianne Wildi
Susan Emmenegger
Fabian Schmid
Cornelia Stengel
Bettina Hürlimann-Kaup
Martin Hess/Stephanie Lienhard
Harald Bärtschi/Nicolas Jacquemart/Stephan D. Meyer

Helbing Lichtenhahn Verlag

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Die Druckvorlagen wurden von der Herausgeberin reprofertig geliefert.

Alle Rechte vorbehalten. Dieses Werk ist weltweit urheberrechtlich geschützt. Insbesondere das Recht, das Werk mittels irgendeines Mediums (grafisch, technisch, elektronisch und/oder digital, einschliesslich Fotokopie und Downloading) teilweise oder ganz zu vervielfältigen, vorzutragen, zu verbreiten, zu bearbeiten, zu übersetzen, zu übertragen oder zu speichern, liegt ausschliesslich beim Verlag. Jede Verwertung in den genannten oder in anderen gesetzlich zugelassenen Fällen bedarf deshalb der vorherigen schriftlichen Einwilligung des Verlags.

ISBN 978-3-7190-4138-0
© 2018 Helbing Lichtenhahn Verlag, Basel
www.helbing.ch

Vorwort

Der Zahlungsverkehr steht im Umbruch. Die technologiegetriebenen Innovationen führen auf dem Markt für Zahlungsdienste fortlaufend zu neuen Produkten, viele davon werden von neuen Anbietern aus dem Nichtbankensektor lanciert. Gleichzeitig verändert sich mit der Zahlungsdiensterichtlinie II (PSD2) der europäische Rechtsrahmen für den Überweisungsverkehr.

Für die Umbruchstimmung steht unter anderem das Stichwort «Open Banking», also die Öffnung der Banken gegenüber Drittanbietern hinsichtlich der Nutzung von Bankdaten. Dass diese Entwicklung nicht nur den Zahlungsverkehr, sondern das Bankgeschäft insgesamt massgeblich verändern wird, steht ausser Frage. MARIANNE WILDI, CEO der «digitalsten Bank der Schweiz» sieht im Open Banking in erster Linie die Chancen – und die Freude, gemeinsam in die Zukunft zu gehen.

SUSAN EMMENEGGER befasst sich mit dem neuen europäischen Rechtsrahmen für die Zahlungsdienste. Die Schweizer Banken haben sich im Rahmen von SEPA zur Beachtung der PSD2 verpflichtet. Sie haben diesbezüglich noch einen gewissen Nachholbedarf. Einen zentralen Eckpunkt der PSD2 bilden die Vorschriften über die (starke) Kundenauthentifizierung. Sie sind nicht nur aufsichtsrechtlich relevant, sondern sie werden mit den zivilrechtlichen Haftungsbestimmungen verflochten. FABIAN SCHMID präsentiert die Rechtslage in der EU und zeigt auf, was sie für die Schweiz bedeutet.

Mit der Disruption im Markt für Zahlungsdienste tritt die Frage nach den Risiken und der Risikotragung bei unautorisierten Transaktionen verstärkt in den Vordergrund. Eine Beitrags-Trias untersucht diesen Themenbereich aus verschiedenen Perspektiven. SUSAN EMMENEGGER richtet den Blick auf die Dritten Zahlungsdienstleister. CORNELIA STENGEL analysiert die zivilrechtliche Haftungslage bei unautorisierten Transaktionen in Zahlungssystemen am Beispiel von Twint. MARTIN HESS und STEPHANIE LIENHARD befassen sich mit unautorisierten Zahlungen im Zusammenhang mit virtuellen Währungen – und versehen ihren Beitragstitel prompt mit einem Fragezeichen!

Ohne Fragezeichen steht demgegenüber der Befund, dass im Zusammenhang mit den virtuellen Währungen zahlreiche Rechtsfragen noch ungeklärt oder jedenfalls umstritten sind. Dazu gehört die Frage, ob Zahlungen in Bitcoins Sachleistungen sind. BETTINA HÜRLIMANN-KAUP gibt darauf eine dezidierte Antwort: Bitcoins sind keine Sachen. Die Frage nach der Vergleichbarkeit von virtuellen und traditionellen Währungen stellt sich zudem

bei den ganz «normalen» Transaktionen. HARALD BÄRTSCHI, NICOLAS JAQUEMART und STEPHAN D. MEYER untersuchen die Rechtslage im Hinblick auf Zahlungen und Zahlungsrückstände, wenn für die Transaktion virtuelle Währungen eingesetzt werden.

Den Referentinnen und Referenten sei an dieser Stelle herzlich gedankt für ihre Bereitschaft, die Wunschthemen der Tagungsleitung aufzugreifen, sich mit ihnen auseinanderzusetzen und ihre Erkenntnisse in den Dialog von Wissenschaft und Praxis, wie er an der SBT stattfindet, einzubringen. Es ist keine Selbstverständlichkeit – Danke! Danken möchte ich auch dem Team des Instituts für Bankrecht für die Organisation dieser Tagung. Ich konnte mich in jeder Phase voll und ganz auf Euch verlassen – herzlichen Dank für den tollen und erfolgreichen Einsatz! Besonders danke ich LESLIE ANN SOMMER und MICHA PROBST für die Federführung bei der Organisation der Tagung. LESLIE ANN SOMMER war darüber hinaus für den Tagungsband verantwortlich, auch dafür ganz herzlichen Dank.

Bern, im Juni 2018 *Susan Emmenegger*

Inhaltsübersicht

Open Banking

Marianne Wildi, Lenzburg*

Inhaltsverzeichnis

I. Einleitung

Einen wunderschönen guten Morgen. Ich muss Sie ein wenig bedauern, weil Sie jetzt das Vergnügen haben, einer Informatikerin/Direktorin zuzuhören. Die Informatikerin schläft am Morgen normalerweise. Wach ist um diese

* Marianne Wildi ist CEO der Hypothekarbank Lenzburg. Beim vorliegenden Text handelt es sich um die Aufzeichnung des mündlichen Vortrags.

Zeit hingegen die CEO der Hypothekarbank Lenzburg. Ich hoffe, Sie haben Verständnis, wenn mein Regtech-Fintech-Herz jetzt vielleicht eher zu Fintech als zu Regtech tendiert. Ich habe grosse Ehrfurcht vor dem wissenschaftlichen und juristischen Know-how, das in diesem Saal vorhanden ist. Ich bin zu Hause oftmals mit Revision, Compliance und Riskmanagement konfrontiert. Entsprechend beeindruckt bin ich über die Fülle der Wissensmacht, die vor mir sitzt und der ich jetzt als kleine Informatikerin die Chancen des Open API Banking frühmorgens – für meine Zeit – präsentieren möchte. Eigentlich will ich Ihnen aber vor allem ein paar Gedanken mitgeben, die Sie vielleicht inspirieren. Die kreativ, die innovativ sind – disruptive Gedanken. Denn diese werden uns durch die schnellen Änderungen leiten und begleiten, die das Bankgeschäft vor sich hat. Ich werde mich kurz zu meiner Bank, der Hypothekarbank Lenzburg, äussern. Anschliessend spreche ich über die Veränderungen und insbesondere zum Banking der Zukunft. Abschliessend sind noch einige Fragen angekündigt worden, die ich gerne beantworten werde.

II. Vorstellung der Bank: 150 Jahre Tradition

Die Hypi ist eine Hypothekarbank im Herzen des Kantons Aargau. Sie werden sich fragen, wie eine vergleichsweise kleine Regionalbank auf die Idee kommt, in der Informatik irgendwas zu bewegen.

Wir haben ganz normale Geschäftsstellen, wie das für eine Regionalbank üblich ist. Wir sind aber börsenkotiert und haben direkte Börsenanschlüsse. Schon das ist ein wenig speziell. Tatsächlich sind wir noch ein bisschen spezieller: Denn wir sind die erste Schweizer Bank, die überhaupt ein Open API, das heisst klar definierte, offene Schnittstellen, zur Verfügung stellt.

Wir sind eine Mischung aus Tradition und Innovation und wir haben das auch in den letzten Jahren so gelebt. Dieses Jahr feiert die Bank ihr 150. Jubiläum. Ich werde Ihnen jetzt nicht die ganze Geschichte der Bank erzählen. Ich möchte mit Ihnen aber einen Blick auf die letzten drei Jahre werfen, als wir unsere Strategie ganz bewusst auf Basis unserer Kultur von Tradition und Innovation gemeinsam mit dem Verwaltungsrat, der Geschäftsleitung und allen Mitarbeitenden definiert haben. Wie wir uns bewegen, und: dass *Open Banking* ein Teil dieser Strategieumsetzung ist.

III. Digitalisierung verändert Wirtschaft und Gesellschaft nachhaltig

Payment Innovation, Hackathons, Banking, Service, Storytelling und so weiter: Mit Hilfe von Wortwolken kann man stundenlang referieren und diskutieren. Wenn Ihnen Wortwolken begegnen, lassen Sie Ihrer Phantasie freien Lauf, studieren Sie, seien Sie kreativ. Die Verbindungen, die man in Wortwolken macht, sind wie künstliche Intelligenz mit neuronalen Netzen. Wie Ihr Hirn, das automatisch funktioniert. Es steckt ein sehr interessantes Geschäftsmodell dahinter, wenn man das alles abbildet – und das nicht nur im Banking: Ökosysteme, Open API, Verbindungen zwischen Industrien, Verbindungen zwischen verschiedenen Branchen. Es ist ein wirklich magisches Werk von API und Verbindungen technologischer Art. Mit allen Risiken, die damit verbunden sind, namentlich hinsichtlich der Sicherheit, des Datenschutzes, der Cybergefahren etc. Bevor ich in diese ernsten Themen eintauche, möchte ich vorab aber das Kreative, das Lustige, das Abwechslungsreiche betonen, das mit diesen Möglichkeiten verbunden ist.

1. Veränderungen in der Wirtschaft

Wenn man über die Landesgrenze schaut, sieht man, was im Zahlungsverkehr alles passieren kann. In den nordischen Staaten erfolgt selbst die Kirchenkollekte elektronisch, per Kreditkarte am Ausgang. Und dass man Bankomaten lange suchen muss, liegt nicht nur daran, dass sie anders heissen. Es gibt schlicht viel weniger davon, dafür findet man viel mehr digitales Geld und andere Möglichkeiten, auf Bargeld zu verzichten. Persönlich habe ich nicht wirklich gerne Handtaschen dabei. Wenn ich in meiner Hand einen NFC Chip hätte und meine Kredit- und meine Debitkarte in meiner Hand oder in meiner Uhr, dann wäre das eine nützliche Dienstleistung. Allerdings sind wir dann wieder bei der Sicherheit und beim Datenschutz. Denn es fragt sich, was der Chip in meiner Hand sonst noch alles kann. Es gibt unzählige interessante Gedanken, spannende Möglichkeiten, um Sachen auszuprobieren und sie auch immer wieder zu hinterfragen. Denn eines ist klar: In Sachen Zahlungsverkehr haben wir zwar Vieles hinter uns. Aber noch mehr kommt erst noch auf uns zu.

Was auf uns zukommt, verändert uns als Wirtschaft, verändert uns als Gesellschaft. Es ist eine fesselnde Mischung aus Menschen, Wirtschaft, Technologien, Komponenten, Verbindungen, Fintech, Banken, etablierten

Firmen, Startups, traditionellen Firmen. Es ist ein innovatives Arrangement von anders zusammengesetzten Wertschöpfungsketten und einzelnen Ausschnitten bestehender Wertschöpfungsketten. Sicher ist auch, dass das Tempo nicht abnimmt, dass der Druck eher steigt, dass das Preisniveau sich tendenziell seitwärts, oder sogar nach unten bewegt. Denn die Konkurrenz ist stark und die Konkurrenz kommt nicht nur aus dem Bankensektor. Das lässt sich auf andere Branchen übertragen. Es gilt für die Printmedien, für den Energiesektor, selbst für das E-Government. Für den Bankensektor, der uns hier am meisten interessiert, steigt gleichzeitig die Bedeutung von Themen wie Datenschutz, Sorgfaltspflichten, Zugang von Dritten zu Bankkonten, Open API und – das alles übergreifend – die ganzen Sicherheitsaspekte.

2. Veränderungen in der Gesellschaft

Wir befinden uns in einer neuen Welt, die sich in sehr hoher Geschwindigkeit präsentiert. Sie erinnert mich ein wenig an die *VUCA World* – eine Welt in ständigem Wandel [Anm.: *VUCA* steht für volatility, uncertainty, complexity, ambiguity]. Die *VUCA World* wird häufig grün dargestellt, das erinnert an die Yucca-Pflanze, das kann man sich leichter merken. Überhaupt hilft es, ein bisschen häufiger bildlich und kreativ zu sein, ein wenig quer zu denken. Sonst kommt man in der heutigen komplexen Welt nicht so schnell voran, wie man sollte. Und das ist letztlich eine Frage des Bewusstseins: Unsicherheit kann man auch positiv verstehen. Unsicherheit kann zum Denken anregen. Dazu motivieren, bewusst etwas zu tun. Aber die *VUCA* World ist sehr volatil, komplex und eben vielschichtig. Gerade deshalb befassen wir uns generell mit extrem spannenden Themenbereichen.

a) Das GAFA-Monopol

GAFA: Die Abkürzung mag nicht allen unter Ihnen geläufig sein. Aber die Firmen, für die sie steht, kennen Sie mit Sicherheit. Es handelt sich um Google, Amazon, Facebook und Apple. Ich gehe davon aus, dass Sie alle heute bereits etwas gegoogelt haben. Vielleicht haben Sie auch *Uber* benutzt, um herzukommen, oder sie haben auf dem iPhone nachgeschaut, mit wieviel Verspätung Ihr Zug ankommt. Die Plattformen sind nicht unbekannt, und mit ihnen all die Risiken, die damit verbunden sind.

Ist das die Welt, in die wir uns hineinbewegen? Das wäre eine überregionale, internationale Welt. Dann wird sich die Hypothekarbank Lenzburg im Herzen des Kantons Aargau als Regionalbank irgendwo hinter

Google, *MSN*, *Facebook*, *Apple* einreihen, weil wir wissen, dass wir uns zu bewegen haben. Sie müssen sich keine Sorge machen: Wir meinen nicht, wir würden das zweite Apple oder das zweite Google. Aber wir sind überzeugt, dass wir fähig sind, uns zu bewegen. Weil wir gar nicht anders können, als uns zu bewegen und über den Tellerrand zu schauen.

b) Disruptive Geschäftsmodelle

Wer hätte vor Kurzem gedacht, dass disruptive Geschäftsmodelle möglich sind? Wir alle kennen ein grosses Taxiunternehmen, das keine Taxis mehr hat. Was würde das für Ihre eigene, die Bankbranche bedeuten? Führt es zur Frage, ob es Banken noch braucht? Das hat Bill Gates vor Jahren schon gesagt und alle haben es oftmals zitiert und nie wirklich geglaubt. Was bedeutet es, wenn Alibaba als weltgrösster Händler keine Lager mehr benötigt? Was bedeutet es, wenn man Softwareverkäufer ist und keine Programme mehr schreibt? Die Dinge haben sich auf eine Art verändert, dass wir uns fragen müssen: Wer überrennt uns und wo rennen wir mit? Wo ist der Ort, wo wir uns in einem Ökosystem noch einfügen können? Oder hoffen wir auf eine Nische, die so super ist, dass im Herzen des Kantons Aargau alle Leute ihr Leben lang noch Bargeld beziehen? Die begeistert sind vom Bargeld, die Interesse haben an der Schalterkasse und am persönlichen Kontakt mit uns Bankmitarbeitenden? Dann ist unsere Welt weiterhin in Ordnung. Vielleicht finden wir diese Nische mitten in Lenzburg, nahe beim Bahnhof und alle kommen bei uns vorbei. Aber vielleicht ist das Leben nicht so. Und das wiederum bedeutet, dass man sich mit den Veränderungen auseinandersetzen muss.

IV. Banking der Zukunft

Was kann mit Banken passieren? Ein mögliches Szenario ist, dass sich nicht viel verändert. Wenn man in Bern ist, lästert man gerne über die FINMA: Sie verschärft ständig die Rahmenbedingungen und schränkt die Geschäftstätigkeit ein. Gleichzeitig betreibt die FINMA Artenschutz. Je mehr Vorschriften, je komplizierter sich die Regulierung präsentiert, je höher die Markteintrittshürden sind, desto besser ist das traditionelle Geschäftsmodell der Banken geschützt. Danke FINMA, weiter so! Wir sind gerne eine Hypothekarbank im Herzen des Kantons Aargau mit einem traditionellen Geschäftsmodell.

Es könnte sein, das die FINMA sich bewegt, weil die Welt sich bewegt. Ich möchte hier kein FINMA-*bashing* machen, denn die FINMA hat sich tatsächlich bewegt. Das Bankgeschäft kann sich nämlich neu erfinden. Es gibt *Rules und Regulations,* die in diese Richtung gehen, aber wir müssen uns damit auseinandersetzen, uns fragen, was das für uns alle heisst.

Es kann bedeuten, dass wir Banken uns neu erfinden müssen – mit Partnerschaften, mit Kooperationen. Die Hypothekarbank Lenzburg arbeitet mit Fintechs zusammen. Das haben wir in letzter Zeit intensiv geübt. Aber das ist noch kein wirklich neues Bankmodell. Es ist einfach eine andere Kombination, wie man Banking auch machen kann. Wir sind immer noch traditionelle Banker. Aber wir sind solche, die versuchen, mit innovativeren Ansätzen etwas in die Wege zu leiten, mit ein bisschen flexibleren Ansätzen etwas zu bewegen. Mit Partnerschaften und Kooperationen, beispielsweise mit Fintechs oder Regtechs. Das effektiv Interessante ist dann wieder das Ökosystem.

1. Ökosysteme

Für Ökosysteme ist die Kooperationsfähigkeit eminent wichtig. Man kann an einem Ökosystem teilnehmen, wenn man flexibel genug ist. Ob das nun ein Ökosystem von Banken, oder eines Energieanbieters oder eines neutralen Anbieters ist, der einfach eine Plattform neu schafft, wo sich ganz viele Kunden zu einer Community vereinen, die wir heute noch nicht kennen.

Vielleicht ist das Ökosystem etwas ganz Anderes und wir Banker müssen schauen, dass wir uns neu erfinden. Oder dass wir uns so flexibel gestalten, dass wir dem einen Kunden das Eine bieten können und im zweiten Segment vielleicht das Andere. Dass wir aber immer ein Teil der Zukunft sein können, sofern es dann die Zukunft wird. Wenn Sie über die Generation Y, Z oder X reden, können Sie sich überlegen, welcher Generation Sie angehören. Möglicherweise noch den Baby-Boomern. Grundsätzlich aber verändern wir uns extrem, unsere Mitarbeitenden sowieso, desgleichen unsere Kunden. Daher muss sich auch unser Bankmodell, unser Geschäftsmodell, immer wieder neu erfinden.

Wenn wir uns bei der Hypothekarbank Lenzburg über Anpassungen des Geschäftsmodells, der IT, von Fintech oder sonstige Veränderungen und Innovationen unterhalten, ist uns bewusst, dass es eine Zusammensetzung, eine Quasiordnung ist. Das ist unser Haus, das zu uns passt, weil es verschiedenste Aspekte umfasst. IT ist nur ein kleiner Zweckbaustein in diesem

Bau – zwar ein relativ zentraler, aber einer, der unserer Organisation und Kultur entspricht. Man kann seine Bank nicht erfolgreich umbauen oder umbauen lassen, wenn man die Bank nicht mitnimmt. Wir können nur gemeinsam mit unseren Kunden und unseren Mitarbeitern diese Zukunft gestalten. Das ist nicht eine reine IT-Geschichte. Es ist eine Geschichte über Innovationskraft, die eng mit der Organisation und Kultur verbunden ist. Mitarbeiter können nur innovativ sein, wenn die Kultur passt. Wenn man eine Kultur hat, die Fehler nicht toleriert, ist man nicht innovativ. Fehler können passieren. Als Anwälte oder Juristen werden Sie wahrscheinlich sagen, dass Fehler nicht passieren dürfen. Das stimmt natürlich, aber das meine ich gar nicht. Ich meine auch nicht, dass man versehentlich oder fahrlässig agieren soll. Ich sage nur, dass man die Kultur haben soll, etwas auszuprobieren und nachher zuzugeben, dass es ein Versuch war und dass das Projekt nicht geklappt hat. Das heisst nicht, dass man nicht die Rahmenbedingungen fixieren muss, um das Risiko zu beschränken und die Sicherheit zu gewährleisten. Wir sind immer noch eine Bank. Aber es heisst, dass man die Gedanken frei laufen lässt, wenn es darum geht, ob man mit Kunden anders umgehen kann. Genau dafür muss man eine IT-Struktur haben, die flexibel genug ist, diese Dinge zu unterstützen und zu lernen, was das für das bestehende Geschäftsmodell heisst.

Aber das Ziel ist – da sind Sie wahrscheinlich mit mir einig –, dass die Kunden es effektiv merken. Wenn die Kunden nicht merken, dass wir uns verändern, dann ist auch irgendwas in der Digitalisierung und in den Innovationen schief gelaufen. Denn die Kunden müssen die überall gerühmte *Kunden-Experience* wirklich geniessen können.

Was wir machen, machen wir nicht alleine. Auch das ist ein Teil davon, wie man sich in einer solchen Welt bewegen soll, kann und muss. Indem man nämlich neue Communities nutzt. Dass man mit Leuten spricht, so wie Sie heute hier sitzen. Digitalisierung ist eigentlich ein Ökosystem, ein Netzwerk. Was wir heute sind oder darstellen, ist auch ein Netzwerk. Es ist ein physisches und ein persönliches Netzwerk. Das heisst: Wir haben im Grunde genommen nur Netzwerke um uns, mit unterschiedlichen Sicherheitsstufen und Verbindungen. In diesen tauschen wir uns auch aus. Heute ist das Netzwerk bunt gemischt: Grosse Banken, kleine Banken, Versicherungsfirmen, Universitäten. Es ist sehr spannend, in diesem Netzwerk dabei zu sein! Es ist interessant, wie offen und konstruktiv man Ideen austauschen kann zu Themen wie Open API, Standardisierung, oder wie Banken beziehungsweise Finanzdienstleister sich verändern können.

Ein zweites wichtiges Netzwerk, wo wir Ideen und Know-how austauschen, ist das Business Engineering Institut in St. Gallen. Im Anschluss an meinen Vortrag werde ich ein Interview mit jemanden machen, der mit Smart Contracts umgehen kann. Denn auch die Hypothekarbank Lenzburg hat ein Blockchain-Projekt, genauer: ein Digital Ledger-Projekt, um etwas auszuprobieren. Und das möchte ich Ihnen auf den Weg geben: Probieren Sie Sachen aus, beachten und beurteilen Sie die Risiken, die Sie eingehen. Aber haben Sie keine Angst, etwas auszuprobieren, zu diskutieren, sich auszutauschen. Denn nur so kommen Sie vorwärts.

2. Open API

a) Strategie

Haben wir Angst vor Open API? Haben wir Angst vor der Öffnung des Marktes? Wir von der Hypothekarbank Lenzburg dürfen keine Angst davor haben. Weil wir uns öffnen können, öffnen dürfen. Wenn man sehr gross ist, vielleicht schon international oder wenigstens schweizweit so dominant ist, dass eine Öffnung Kundenverluste bringen könnte, ist man möglicherweise vorsichtiger mit dem Entscheid, ob man sich öffnen will. Als Regionalbank können wir uns aber problemlos öffnen, denn wir können von einer offenen Gesellschaft, einer offenen Community, einer offenen Plattform, einem Ökosystem profitieren. Für uns ist Open Banking eine Chance, mit Kooperationspartnern etwas zu bewegen. Eine Chance, dass wir nicht jedes Rad neu erfinden müssen, und stattdessen mit bestehenden Rädern und Modulen für unsere Kunden arbeiten können. Wie wir das zusammensetzen, das wollen wir mit Hilfe eines offenen Ansatzes orchestrieren.

Die Funktionsweise dieses offenen Ansatzes ist eine Mischung von verschiedensten Kombinationen. Angefangen mit der Swiss Fintech Innovation Gruppe (SFTI), die sich mit dem Open API befasst. Es ist ein Austausch zwischen Banken im Interesse der Kunden. Der Kunde steht im Mittelpunkt, er kann steuern. Das ist aber nur der Anfang der Geschichte. Sie endet nicht hier, sondern sie geht in die branchenübergreifenden Themen weiter. Wenn man sich die Mühe nimmt, bei der Energie oder anderen Branchen mitzuhören, dann sieht man, dass diese Branchen Netzwerke beziehungsweise Ökosysteme bauen. Auch als Bank muss man schauen, dass man sich zu Netzwerken verbindet. Dann ist man noch dabei, andernfalls ist man bald verschwunden. Weil irgendein grosser Service Provider aus der Industriebranche die Abwicklungen anbieten wird. Wir als Banken müssen schauen, dass

wir in andere Ökosysteme hineinkommen. Wir müssen fähig sein, Ökosysteme zu unterstützen. Wir müssen die eigenen Service orchestrieren können. Kurz: Wir müssen fähig sein, unsere Kunden auf der berühmten Customer Journey zu begleiten. Das endet in anderen Geschäftsmodellen, mit anderen Ansätzen.

b) Beispiel: Der virtuelle Bankautomat

Ein Beispiel für ein anderes, neues Service-Modell ist der virtuelle Bankautomat. Man kann sagen: So etwas braucht es nicht, es gibt schon genügend Bankautomaten und die Gesellschaft will sowieso bargeldlos bezahlen. Wer kommt denn auf die komische Idee, noch Bankautomaten einzuführen? Wer braucht überhaupt noch Bargeld? Das sind Themen, über die man stundenlang diskutieren könnte. An diesem speziellen Fall war für uns interessant, dass wir einen Fintech gefunden haben, der erstens keinen Finanzierungsbedarf hatte, der zweitens schon über ein Geschäftsmodell, einen *Business* Case, verfügte, und der drittens schon Werbemittel zur Verfügung hatte, um etwas zu bewirken. Wir hatten also einen Fintech, der schon so weit war, dass er wirklich in der Schweiz ein Open API gesucht hat. Daraus resultierte eine Win-Win-Situation für uns und für den Fintech.

Der Kunde profitiert von diesem Angebot. Wenn er beispielsweise Apotheker oder ein Bäcker ist, also ein traditioneller Kunde von Regionalbanken, kann er Bargeld auszahlen. Das heisst, es kommen jetzt Menschen zum Apotheker oder zum Bäcker, um sich mit Bargeld zu versorgen. Natürlich kaufen sie noch etwas Anderes. Aber grundsätzlich animieren wir damit einen Traffic: Die Leute gehen wieder in die Läden, die Leute holen Bargeld. Es sind unsere Kunden, weil es direkt ihrem Konto belastet wird. Was aber viel wichtiger ist: Unser Open API funktioniert in der Produktion. Das war aus unserer Sicht das Zentrale. Dass es darüber hinaus für alle anderen Beteiligten auch noch eine Success Story wurde, ist natürlich super. Für uns aber war wichtig, dass wir zeigen konnten, dass wir über unser Open API tatsächlich Anbindungen in der Produktion, im Life-Betrieb anbieten können – und zwar nicht nur über das traditionelle E-Banking, das jeder kennt.

3. Chancen und Risiken

Open API: Das sind Chancen und Herausforderungen. Die Herausforderungen, zum Beispiel das Cyberrisiko, kennen wir bestens. Aber man muss auch über die Chancen reden. Es sind Chancen auf veränderte Kostenmodel-

le. Es sind Chancen, sich die notwendige Flexibilität aufzubauen. Zum Beispiel die Flexibilität, mit einer anderen, jüngeren Kundengeneration umzugehen und dort eine neue Kundenerfahrung anzubieten. Das kann man relativ einfach, wenn man – wie wir – als Bank sein eigenes System orchestriert. Denn dann kann man das, was man über das Open API integriert, auch im E-Banking zur Verfügung stellen.

So war das zum Beispiel beim Personal Finance Manager. Auch das ist ein Tool, das man über Open APIs relativ einfach anschliessen kann. Wir haben ein PFM-Tool eines Fintech in unser E-Banking eingebunden und es gibt eine Applikation, eine separate App, die dieses Produkt verwendet. Was ich damit ausdrücken will: Es ist wichtig, dass man die Synergien in einem Netzwerk auf den verschiedensten Kanälen nutzen kann. Denn es ist nicht klar, welcher Kanal am Schluss überlebt.

Wenn man das Management – also das Orchestrieren der Kanäle – wirklich verantworten will, muss man die Dienstleistungen beherrschen und sie sicher machen können. Bei dieser ganzen Faszination von Technologie im Open API oder im Open Banking darf man nicht vergessen, dass es um Sicherheit und insbesondere um Datenschutz geht. Was passiert mit den Kundendaten? Merkt der Kunde, der sich auf verschiedenen Kanälen bewegt, überhaupt noch, was mit seinen Daten passiert? Wissen wir als Bank, was der Kunde mit seinen Daten macht? Oder meint der Kunde immer noch, es seien unsere Daten? Sind es überhaupt je unsere Daten gewesen?

Als Bank muss man sich ganz explizit damit auseinandersetzen, für wen welche Zugriffsrechte bestehen bzw. welche Authentifizierungs- und Autorisierungsprozesse zum Einsatz kommen. Wie viele Faktoren soll der Kunde zum Einloggen in sein E-Banking, seine neue Finanz-App oder was auch immer die App dann macht, verwenden müssen? Die jüngere Generation ist diesbezüglich manchmal etwas unvorsichtiger – heute sagt man: *convenient*. Es ist sehr bequem, einfache Prozesse spielerisch zu gestalten. Aber am Schluss geht es immer um Geld, um das Bankgeschäft. Das heisst: Wir müssen etwas verbinden, das wir aus der Sicht des E-Banking gut kennen: Firewalls, Security Steps, Zugriffsberechtigungen. All das muss auf die Open-API-Geschichte adaptiert werden. Es muss alles genau so sicher wie das E-Banking heute sein. Es ist dieselbe Herausforderung, nur ist sie grösser geworden, weil viel mehr Players und viel mehr Komponenten betroffen sein können, wenn irgendwo Daten verloren gehen oder attackiert werden.

Die Cybersicherheit ist ein extrem wichtiges Thema und man muss lernen, welche Sicherheitsmechanismen man zusätzlich einbauen kann; bei-

spielsweise auf den Systemen der Bank mit der Fraud Detection. Welche Verhaltensmuster sind normal für diesen Kunden, welche nicht? Es gibt viele Tools, die Verhaltensgrundlagen oder Verhaltensmuster der Daten analysieren. Es ist extrem interessant, was man technologisch alles machen kann. Aber es ist ganz wichtig, das der Mensch noch wissen muss, was am Schluss daraus resultiert. Weil nur der Mensch am Schluss die zusätzliche Sicherheit gewährleistet. Der Mensch muss mitdenken. Die Technologie ist wichtig, sie ist die Grundlage, aber der Mensch muss studieren. Wenn der Mensch – sei es der Kunde, der Banker, der Fintech-Anbieter – nicht mitdenkt, dann ist das System zu unsicher. Der Mensch ist immer noch das grösste Risiko, auch beim Thema Open Banking.

V. Fazit

Ich sehe vor allem Chancen. Die Chance, das Open API Banking ins Leben zu rufen oder am Leben zu erhalten. Zu kooperieren, Informationen auszutauschen, Module auszutauschen, das Rad nicht neu zu erfinden – und bei alledem das modulare System so zu kontrollieren, dass wir unser Angebot für unsere Kunden, passend auf unsere Bankberater, passend auf das, was wir gut können, anbieten – mit der flexiblen, innovativen, coolen *Experience*, mit all den Erlebnissen, die wir bieten wollen.

Klar ist aber auch: Digitalisierung ist nicht nur Erlebnis, nicht nur Spass, nicht nur lustig, nicht nur farbig, nicht nur *Gamification.* Digitalisierung bedeutet auch, dass man – wenn man schon alle Prozesse anschaut – das Potential bezüglich Sicherheit und Datenschutz ausschöpft. Wenn Sie schon alles anschauen dürfen, packen Sie die Chance, Ihre Prozesse auch zu überarbeiten und sich wirklich modern aufzustellen, damit Sie in den Ökosystemen der heutigen Zeit dabei sein können: Sicher, flexibel, agil. Ich bin überzeugt, dass wir so die Chancen packen und wirklich neue Kundenerlebnisse schaffen – und am Schluss vielleicht im bestehenden Modell glücklich sind oder eben mit unseren Kunden in ein anderes, verändertes Geschäftsmodell überführt werden. Open Banking ist für mich nicht eine Technologie sondern ein Denkansatz, es ist vor allem Open Thinking. Es ist eine Art und Weise, wie sich unsere Bank, unsere Mitarbeiter, wir alle zusammen – Verwaltungsrat, Geschäftsleitung, Mitarbeitende, Kunden, Aktionäre – in die Zukunft bewegen. Und dies auf der Basis von Tradition und Stabilität. Wir wissen, was wir tun und wir wissen, in welche Richtung wir gehen. Weil wir

wissen, dass Digitalisierung und Innovation auch die Freude ist, gemeinsam in die Zukunft gehen.

Anhang: Open Banking: Interview

Interview mit Marianne Wildi[*] zum Thema Open Banking,
durchgeführt von Eleonor Gyr[**]

Eleonor Gyr: Vielen Dank Frau Wildi für Ihr spannendes Impulsreferat. Im Bankensektor findet seit Längerem eine Konsolidierung statt und auch im Zusammenhang mit der neuen Finanzmarktgesetzgebung, Stichwort Fidleg, werden kleinere Institute totgesagt. Ist Digitalisierung oder im Speziellen Open Banking eine Chance für kleine Institute, sich am Markt zu behaupten?

Marianne Wildi: Es muss nicht unbedingt die Digitalisierung sein. Aus meiner Sicht geht es darum, dass man komplexe Probleme mit Partnerschaften und Kooperationen besser löst. Das ist die Philosophie von «open», also von Offenheit. Wir haben beispielsweise in der Umsetzung des Fidleg mit einem Fintech kooperiert, der bei uns nicht den Kundenteil, also den «Experience-Teil» abdeckt, sondern die Risikokennzahlen. Auch in diesem Bereich kann man durch Kooperationen und intelligente Schnittstellen voneinander profitieren. «Open» bedeutet die Chance, einen Prozess zu orchestrieren und für diesen Prozess auf fremde Ressourcen zurückzugreifen. Das ist eine Chance des Open Banking. Aber eigentlich ist es eine Chance der Philosophie der Offenheit. So, wie Sie wahrscheinlich die PSD2 juristisch verstehen, ist Open Banking ein wenig enger gefasst. Technologisch gesehen ist Offenheit für mich weiter gefasst. Was aber sicher ist: Offenheit ist und bleibt eine Chance, auch für kleine Institute.

---

[*] Marianne Wildi ist CEO der Hypothekarbank Lenzburg.

[**] Eleonor Gyr ist Rechtsanwältin und wissenschaftliche Mitarbeiterin am Institut für Bankrecht der Universität Bern. Sie forscht zum Thema der Smart Contracts.

Eleonor Gyr: Sehen Sie darin gerade den Grund, wieso eine kleine Bank wie die Hypothekarbank Lenzburg eine Vorreiterrolle spielt und nicht eines der grossen bekannten Institute am Markt?

Marianne Wildi: Wir haben historisch gesehen den Vorteil, dass wir der Zeit ein bisschen voraus unterwegs sind. Wir haben schon relativ lange keinen CEO mehr, der ein typischer Kommerzdirektor ist – obwohl wir eine Regionalbank sind. Unser letzter Kommerzdirektor wurde irgendwann im letzten Jahrhundert pensioniert. Der Nachfolger des Kommerzdirektors war ein Betriebswirtschaftler, aber er war im letzten Jahrtausend tätig. Bei der Hypothekarbank Lenzburg hatten meine Kollegen dann das Vergnügen, mich als IT-Menschen als Direktorin zu bekommen. Das macht am Schluss das aus, was wir sind. Wir sind ein bisschen «anders» unterwegs, ein bisschen kreativer. So war das schon immer und das ist wahrscheinlich eine Kulturfrage; auch des Verwaltungsrats, der überhaupt riskiert, eine Informatikerin an die Spitze einer Regionalbank zu stellen. Rechtzeitig, als die Digitalisierungswelle kam. Diese Chance haben wir gepackt.

Eleonor Gyr: Sie haben die Haftungsrisiken erwähnt. Haben Sie Ihre Compliance- und Rechtsabteilung mit der Lancierung des Open Banking verdoppelt oder verdreifacht?

Marianne Wildi: Ich habe verschiedene Kollegen in diesem Raum, wir haben dieses Thema sehr intensiv diskutiert. Unsere Vision ist, dass man diese verschiedenen Kompetenzen auch im Zusammenhang mit Regtech einfliessen lässt. Das Ziel ist, dass man die Tools nutzen kann, um dann die Menschen dort einzusetzen, wo sie wirklich sinnvoll sind. Dass wir nicht repetitive Arbeiten machen müssen. Dass wir nicht Arbeiten machen müssen, nur weil sie auf einer Checkliste aufgeführt sind. Wir möchten ein neues System erarbeiten. Wir haben vor, den Übergang vom traditionellen Compliance-Teil zu einem moderneren Compliance-Ansatz zu realisieren, der über die first, second und third line of defence wirklich optimal funktioniert. Wir möchten auch hier unsere Frontleute stärker einbeziehen. Um am Schluss die interessante Arbeit nicht durch die Anzahl an Mitarbeitenden, sondern durch die Anzahl an spannenden Aufgaben zu verbessern. Dafür arbeiten wir die verschiedensten Themen auf: Wie man mit Technologien besser unterstützt, wie man besser automatisiert, wie man Prozesse besser steuert. Dann brauchen wir nicht mehr Leute. Auch hier greifen wir auf ein breit abgestütztes Netzwerk von externen Experten, die wir einbeziehen, zurück. Wir meinen nicht, dass wir alles selber erfinden müssen. Wir kombinieren die Erfahrung und

das Know-how aus unterschiedlichsten Quellen. Aber wir orchestrieren intern selber.

Eleonor Gyr: Eine letzte Frage, die vor allem uns junge Juristinnen und Juristen sehr interessiert. Denken Sie, dass ein Verständnis von IT oder gar ein vertieftes Verständnis von IT auch für Juristen notwendig ist? Sollten wir das in unserer Ausbildung mitbekommen?

Marianne Wildi: Ja, IT-Kompetenzen bei den Juristen würde allen Informatikern und überhaupt ganz vielen Mitarbeitern, auch den CEOs, bei der Übersetzung der Anforderungen helfen. So, wie ich es begrüssen würde, wenn mehr Leute in der Bank ein gewisses Grundverständnis von IT hätten. Aber das ist auch bei den Bankfachausbildungen so. Ich denke, das wird sowieso auf uns zukommen, weil wir uns angesichts von Big-Data mit andern Arten von Fragen auseinandersetzen müssen. Das ist bei den Juristen nicht anders. Die Juristen haben den grossen Vorteil, dass Recht schon etwas sehr Analytisches ist – und IT hat sehr viel mit Analytik zu tun. Ich freue mich, wenn Sie alle zu IT-Menschen werden. Und ich hoffe, dass sie alle bei unseren Regtech-Initiativen mitmachen. Unseren Chief Compliance Officer finden Sie auf allen Social Media – please contact him! Aber auch unsere interne Revision ist eigentlich nur bei uns, weil es so spannend ist, in diesem Umfeld dabei zu sein. Wir machen das Ganze wirklich gemeinsam, wir bringen alle unsere Kompetenzen ein und wir lernen zusammen. Um nochmals auf Ihre Frage zurückzukommen: Ja, lernen Sie es auch, denn es macht wirklich Freude, das Geschäft so zu verändern, gemeinsam mit allen Aspekten. Denn noch einmal: Veränderungen passieren nur, wenn alle Funktionen und alle Kompetenzen mitziehen.

PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister

Susan Emmenegger*

Inhaltsverzeichnis

* Prof. Dr. iur., LL.M., ordentliche Professorin an der Universität Bern, Direktorin des Instituts für Bankrecht.

I. Einführung

Seit dem 13. Januar 2018 gilt in der EU die zweite Zahlungsdiensterichtlinie, besser bekannt unter ihrem englischen Namen, *Second Payment Services Directive, PSD2.*[1] Ihr Ausgangspunkt bildet der europäische Binnemarkt als Grundbaustein der Europäischen Union: Ein Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren und Dienstleistungen gewährleistet ist.[2] Der Binnenmarkt sprengt die Grenzen nationalstaatlicher Räume, er impliziert als Ziel einen intensiveren Markt und damit verbunden ein grösseres Wirtschaftswachstum.

Damit sich freie Verkehr von Waren und Dienstleistungen effektiv entfalten kann, müssen die damit verbundenen Geldleistungen effizient abgewickelt werden können. Es braucht also einen funktionierenden Zahlungsverkehr.[3] Die EU hat in diesem Zusammenhang verschiedene Massnahmen ergriffen. Zu den wichtigsten gehören:[4]

– Der flächendeckende Zugang zu einem Zahlungskonto. Verwirklicht wird dies mit der Zahlungskontenrichtlinie.[5] Sie will sicherstellen, dass alle

1 Richtlinie (EU) 2015/2366 vom 25. November 2015 über Zahlungsdienste im Binnenmarkt […] (ABl Nr. L 337 v. 23.12.2015, S. 35).

2 Siehe Art. 26 Abs. 2 AEUV.

3 So bereits das Weissbuch der Kommission an den Europäischen Rat, KOM(85) 310 endg., Rz. 125: «Freizügigkeit, freier Waren- und Dienstleistungsverkehr setzen im übrigen voraus, dass Unternehmen und Privatpersonen überall in der Gemeinschaft Zugang zu gut funktionierenden Finanzdienstleistungen haben.» In diesem Sinne auch LINARDATOS, WM 2014, S. 300.

4 Siehe dazu auch die Übersicht bei BÖGER, Neue Rechtsregeln, S. 195 ff.; HESS, Euro-Zahlungen, S. 54 ff.

5 Richtlinie 2014/92/EU vom 23. Juli 2014 über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen (ABl Nr. L 257 v. 28.08.2014, S. 214). Zur Richtlinie siehe

Verbraucher[6] Zugang zu einem Zahlungskonto mit grundlegenden Funktionen haben.[7] Weiter zielt die Richtlinie auf die Verbesserung der Transparenz von Entgelten für Zahlungskonten für Verbraucher, namentlich durch Informationspflichten und Vergleichswebsites.[8] Zur Förderung des Wettbewerbs werden Zahlungsdienstleister zu Unterstützungsleistungen verpflichtet, damit dem Verbraucher der Wechsel von Zahlungskonten erleichtert wird.[9]

– Die rechtliche Gleichwertigkeit von Bar- und Buchgeldzahlungen. Der Wettbewerb für Waren und Dienstleistungen im gesamten Binnenmarkt kann nur gelingen, wenn Waren und Dienstleistungen im Fernabsatz bezogen werden können. Das wird erreicht durch eine weitgehende Entgeltfreiheit von Buchgeldzahlungen im Valutaverhältnis, die dem faktischen Status quo bei Bargeldzahlungen entspricht. Geregelt wird dies in der Verordnung zu den Interbankentgelten bei Kartenzahlungen[10] und der SEPA-Verordnung.[11] Letztlich spielt hier aber auch die PSD2 eine Rolle, denn sie schreibt in Art. 62 Abs. 4 vor, dass der Zahlungsempfänger keine Entgelte für die Nutzung von Kartenzahlungen sowie bei Überweisungen und Lastschriften verlangen kann.[12] Er darf also seine eigenen Kosten nicht auf den Zahler abwälzen.

LINARDATOS, WM 2015, S. 755 ff. Zur Umsetzung in Deutschland siehe FINDEISEN, WM 2016, S. 1765 ff.

6 Die europäischen Rechtsakten (und auch das deutsche und österreichische Recht) benutzen den Begriff «Verbraucher». In der Schweiz wird dagegen primär der Begriff «Konsument» verwendet. Da es sich hier um einen Beitrag über ein europäisches Regelwerk handelt, wird grundsätzlich der Begriff «Verbraucher» verwendet.

7 Siehe Art. 16 ff. sowie EG 36 ff. der Zahlungskonten-RL.

8 Art. 1 Abs. 1 sowie Art. 3 ff. der Zahlungskonten-RL.

9 Art. 9 ff. der Zahlungskonten-RL.

10 MIF-VO: Verordnung (EU) 2015/751 vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (ABl Nr. L 123 v. 19.05.2015 S. 1). Zur MIF-Verordnung siehe OECHSLER, WM 2016, S. 540 ff.

11 Zur SEPA-Verordnung siehe weiter unten im Text.

12 Art. 62 Abs. 4 PSD2. Die Vorschrift gilt für Zahlungen im Bereich der VO-Interbankenentgelte und der SEPA-VO. Siehe dazu OMLOR, ZIP 2016, S. 561, wonach dies positiv gewendet bedeutet, dass «der Zahlungsempfänger keine Entgelte mehr für Kartenzahlungen sowie für jegliche Überweisungen und Lastschriften erheben» darf. Siehe zum Surcharging und der deutschen Umsetzung in § 270a BGB auch OMLOR, WM 2018, S. 941 f.

– Die preisliche Gleichbehandlung von Inland- und Auslandzahlungen. Diesem Ziel ist die Verordnung über die grenzüberschreitende Zahlungen verpflichtet.[13]
– Die Entwicklung von einheitlichen Standards und technischen Anforderungen für Überweisungen und Lastschriften in Euro. Das wird mittels der SEPA-Verordnung gewährleistet.[14]

SEPA ist allerdings mehr als nur eine Verordnung. SEPA steht für *Single Euro Payments Area,* den einheitlichen Euro-Zahlungsverkehrsraum.[15] SEPA soll die Unterschiede zwischen nationalen und grenzüberschreitenden bargeldlosen Euro-Zahlungen eliminieren. Diese Zahlungen sollen nach denselben Standards und gleich sicher und effizient wie im innerstaatlichen Bereich von irgendwo im SEPA-Gebiet ausgelöst und empfangen werden können.[16]

Die PSD2 spielt im SEPA-Projekt eine zentrale Rolle.[17] Sie schafft ein einheitliches Aufsichtsregime für die Anbieter von Zahlungsdienstleistungen. Sie schafft zudem einheitliche Rechte und Pflichten im Zahlungsdiensteverträg zwischen dem Anbieter von Zahlungsdienstleistungen (vereinfacht: der Bank) und den Nutzern von Zahlungsdienstleistungen (vereinfacht: den Bankkunden).[18] Dieser Vertrag ist in der PSD2, wie schon in der Vorgänger-

13 Verordnung (EG) Nr. 924/2009 vom 16. September 2009 über grenzüberschreitende Zahlungen in der Gemeinschaft und zur Aufhebung der Verordnung (EG) Nr. 2560/2001 (ABl Nr. L 266 v. 09.10.2009, S. 11). Zur Gesetzgebungsgeschichte des EU-Überweisungsrechts siehe WERNER, WM 2014, S. 243 ff.

14 Verordnung (EU) Nr. 260/2012 vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl Nr. L 94 v. 30.03.2012, S. 22).

15 Zur Geschichte von SEPA siehe das (sehr lesenswerte) Buch von WANDHÖFER, EU Payments Integration, passim. Siehe weiter WERNER, WM 2014, S. 243 ff.

16 Ausführlich zu SEPA HESS, Euro-Zahlungen, S. 60 ff.

17 Dasselbe galt bereits für die PSD1, siehe hierzu WANDHÖFER, EU Payments Integration, S. 33 ff.

18 Zu anderen Leitmotiven der PSD2 siehe OMLOR, ZIP 12/2016, S. 559 f.: Förderung des Binnenmarktgedankens und Förderung der Vollendung eines integrierten Marktes für bargeldlose Zahlungen; rechtliche Gleichwertigkeit von Bargeld und Buchgeld; Ausrichtung auf den digitalen Zahlungsverkehr; verbesserter Verbraucherschutz.

richtlinie von 2007,[19] als Verbraucherschutzvertrag ausgestaltet. Das zeigt sich auch daran, dass die Risiken für Bankkunden weiter abgebaut wurden, indem die Haftungsregelungen den Grossteil der Risiken für unautorisierte Zahlungen den Banken zuweisen.

Eine Revision der PSD1 wurde notwendig, weil die Digitalisierung den Zahlungsverkehr in den letzten Jahren grundlegend verändert hat. Heute bezahlen wir im Wesentlichen elektronisch; entsprechend sind neue Sicherheitsstandards notwendig. Die Digitalisierung hat aber auch viele neue Anbieter hervorgebracht, die im Gegensatz zu den Banken als traditionelle Zahlungsdiensteanbieter nicht reguliert sind. Die PSD2 reguliert diese Anbieter, die sogenannten Dritten Zahlungsdienstleister.

II. Relevanz der PSD2 für Schweizer Finanzdienstleister

Warum besteht in der Schweiz Anlass, sich mit der PSD2 zu beschäftigen? Die Schweiz ist nicht Mitglied der EU; die vorgenannten Regelwerke sind in der Schweiz also nicht geltendes Recht und es besteht auch kein Umsetzungszwang. Zudem hat sich die Schweizerische Bankiervereinigung in ihrem Positionspapier vom September 2017 dagegen ausgesprochen, eine PSD2-äquivalente Regulierung einzuführen.[20] Der Fokus des Positionspapiers richtet sich auf einen – allerdings durchaus zentralen Punkt – der PSD2, nämlich die Verpflichtung der Banken, sich gegenüber Drittzahlungsdienstleistern zu öffnen. Die SBVg macht im Wesentlichen geltend, eine Regulierung sei erstens *unnötig,* weil kein Handlungsbedarf bestehe, da die Banken schon heute zahlreiche innovative Lösungen anbieten; ein regulatorischer Zwang zur Öffnung der Banken gegenüber Drittanbietern sei ein unnötiger Eingriff in einen funktionierenden Markt und würde zu Wettbewerbsverzerrungen zu Ungunsten der Banken führen. Zweitens sei eine erzwungene Öffnung gefährlich, weil sie zu *Sicherheitslücken* führen könne. Drittens würden auf Seiten der Bank *zusätzliche Aufwände und Kosten* in den

[19] Richtlininie 2007/64/EG vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (ABl Nr. L 319 v. 5.12.2007, S. 1).

[20] SBVg, Positionspapier (PSD2), September 2017.

Bereichen Sicherheitsstruktur und Compliance entstehen, die letztlich die Kundinnen und Kunden bezahlen müssten.[21]

Die Beschäftigung mit der PSD2 anlässlich einer *Schweizerischen* Bankrechtstagung rechtfertigt sich aber dennoch aus verschiedenen Gründen:[22]

1. Wettbewerb, technische Standards und europäische Kunden

Relevant ist die PSD2 für die Schweizer Banken *erstens* aus Wettbewerbsgründen. Die Schweiz ist ein führender Finanzplatz, der geographisch im Herzen von Europa liegt. Die Schweizer Banken haben deshalb gute Gründe, bei den Rahmenbedingungen des Zahlungsverkehrs mit den Konkurrenten aus dem EU-Raum Schritt zu halten.

Zweitens spielt die PSD2 für die Schweizer Banken sowohl aus aufsichtsrechtlicher als auch aus privatrechtlicher Perspektive eine Rolle, weil sie technische Standards setzt. Wenn die EU im Rahmen der PSD2 Sicherheitsstandards für das Online-Banking und für die Schnittstellen der Banken zu externen Dienstleistern festlegt, dann ist dies eine Regelung zu den operationellen Risiken der Bank. Die FINMA wird solche Standards zur Kenntnis nehmen. Wenn es das Rad schon gibt, muss man es nicht neu erfinden. Man kann es mit weniger Speichen versehen, man kann es kleiner oder grösser machen. Das Rad selber ist aber schon da und es definiert die Ausgangslage für die weiteren regulatorischen Überlegungen, die sich eine schweizerische Aufsichtsbehörde machen wird – spätestens nach dem nächsten publikumswirksamen Hackerangriff auf Kundenkonten. Für das Privatrecht gilt Entsprechendes: Wenn es neue Sicherheitsstandards für das Online-Banking gibt, dann indizieren diese Standards die geschäftsübliche Sorgfalt der Bank – und zwar auch einer *Schweizer* Bank. Es ist dann eben der Standard, der auf den europäischen Finanzplätzen gilt. Das schliesst die Schweiz mit ein.

Drittens ist die PSD2 für Schweizer Banken relevant, weil im Streit zwischen einem EU-Kunden und der Schweizer Bank die PSD2 regelmässig zur

---

21 SBVg, Positionspapier PSD2, September 2017, S. 1. Zusammengefasst lautet das Fazit der SBVg wie folgt: «Eine einseitige Öffnung der Zugriffsrechte für Dritte, wie es die PSD2 innerhalb der EU verlangt, ist ein *Experiment auf Kosten der Bankkunden, das gefährliche Verwirrung schafft und die Datensicherheit der Kunden untergräbt*.» (Hervorhebung im Original). *Id.*, S. 1.

22 Im Ergebnis gleich SCHMID, Starke Kundenauthetifizierung, S. 83 f.

Anwendung kommen wird.[23] Im Retailbereich sind Verträge der Schweizer Bank mit ihren EU-Kunden Verbraucherverträge im Sinne des Lugano-Übereinkommens. Aufgrund des zwingenden Verbrauchergerichtsstandes können die EU-Kunden gegen die Schweizer Bank an ihrem Wohnsitz in der EU klagen,[24] sofern die Bank ihre Tätigkeit auf diesen Staat ausgerichtet hat – wobei die Gerichte und der EuGH die Hürden ausserordentlich tief legen. Ist das Gericht in einem EU-Mitgliedstaat mit der Sache befasst, kommt es aufgrund der Günstigkeitsregel in der Rom I-Verordnung zur Anwendung des nationalen Rechts des mit der Sache befassten Mitgliedstaates – und damit zur Anwendung der (national umgesetzten) PSD2. Auch die Günstigkeitsregel ist zwingendes Recht; anderslautende Rechtswahlklauseln in den AGB der Schweizer Banken sind unbeachtlich. [25] Der Streit des Drogeriekönigs und Multimillionärs Erwin Müller gegen die Bank Safra Sarasin hat diesbezüglich reichlich und für die Banken unangenehmes Anschauungsmaterial geliefert.[26].

---

23 Siehe EMMENEGGER/FRITSCHI, Schweizer Banken: EU-Recht für EU-Kunden, S. 75 ff.

24 Art. 17 i.V.m. Art. 23 Abs 5 LugÜ.

25 Unter dem Günstigkeitsprinzip (Art. 6 Abs. 2 Rom I-VO) ist die Rechtswahl ausgeschlossen, wenn im Staat des gewöhnlichen Aufenthaltes des Verbrauchers Bestimmungen gelten, deren Schutzniveau höher ist als im gewählten Recht. Angesichts des hohen Verbraucherschutzniveaus bei Finanzdienstleistungen in der EU wird damit die Anwendbarkeit des Schweizer Rechts faktisch ausgeschlossen.

26 Siehe EMMENEGGER/FRITSCHI, Schweizer Banken: EU-Recht für EU-Kunden, S. 76 ff. In Kürze: Müller erlitt im Zusammenhang mit den skandalträchtigen Cum-Ex-Geschäften einen (Total-)Verlust von EUR 50 Mio, worauf er die Bank an seinem Wohnsitz in Ulm verklagte. Die Zuständigkeit wurde vom BGH bereits bejaht. Das LG Ulm hat mittlerweile entschieden, die Rechtswahlklausel zugunsten der Schweiz sei ungültig. In Anwendung deutschen Rechts hat es die Bank zur Rückabwicklung des gesamten Geschäfts und damit zur Rückzahlung der Investition verpflichtet, weil die Bank Erwin Müller nicht rechtsgenügend über den Erhalt von Retrozessionen aufgeklärt hatte. Zu den bisherigen Entscheiden siehe BGH, XI ZR 223/15 vom 26. Juli 2016, zusammengefasst in EMMENEGGER/THÉVENOZ, SZW 2017, S. 242, r36. Vorentscheid des OLG Stuttgart zusammengefasst in EMMENEGGER/THÉVENOZ, SZW 2015, S. 410, r39. Sachentscheid: LG Ulm, 4 O 66/13 vom 22. Mai 2017 (Urteilstenor). Zusammenfassung des Entscheides bei EMMENEGGER/THÉVENOZ, SZW 2018, S. 207 r31.

2. Single Euro Payments Area (SEPA)

SEPA spielt für die Schweiz im Zusammenhang mit der PSD2 eine besondere Rolle.[27] Denn die Schweizer Banken nehmen seit 2007 an der technischen Seite von SEPA teil und führen Euro-Zahlungen nach den SEPA-Standards durch. Die Teilnahme an einem technisch einheitlichen Zahlungssystem für Euro ist für die Schweizer Banken zentral, weil damit der Aufwand für Euro-Überweisungen reduziert werden kann. Die Teilnahme an SEPA ist auch faktische Voraussetzung für die Nutzung des EBA-Clearings, also der Clearing-Dienste der European Banking Association. Das EBA-Clearing ist kostengünstiger und schneller und verlangt weniger Liquidität – auch dies ist ein Vorteil für die teilnehmenden Banken.

Die technische Seite von SEPA ist allerdings kein rechtsfreier Raum: Die Schweizer Banken haben sich im Zuge ihres SEPA-Beitritts verpflichtet, die Bestimmungen der PSD2 (und vorher der PSD1) im Bank/Kundenverhältnis zu beachten.

a) Die Akteure

Damit SEPA verwirklicht werden kann, braucht es entsprechende *rechtliche* Rahmenbedingungen. Es braucht aber auch die *technische* Entwicklung eines Zahlungsverkehrssystems, das nach einheitlichen Standards funktioniert; es braucht also Prozesse, Datenformate und Softwarelösungen – kurz: SEPA-Produkte. An der Bereitstellung dieser Rahmenbedingungen sind drei Akteure beteiligt: Erstens die EU-Kommission, welche die rechtlichen Rahmenbedingungen schafft. Zweitens der European Payments Council (EPC), also die Organisation der Kreditinstitute und Branchenverbände. Sie sollen SEPA auf der technischen Seite verwirklichen. Und schliesslich das Eurosystem, also der Zusammenschluss der Euro-Zentralbanken mit der EZB. Das Eurosystem formuliert in enger Abstimmung mit der EU-Kommission die Erwartungen an den ECP hinsichtlich der Umsetzung des SEPA-Prozesses. Die Arbeiten der drei Akteure sind eng verzahnt.

---

[27] Ausführlich WANDHÖFER, EU Payments Integration, S. 33 ff.; HESS/KEISER, SZW 2009, S. 153 ff.; HESS, Euro-Zahlungen, S. 60 ff.

aa) Die EU-Kommission und das Eurosystem

Von der EU-Kommission kam der eigentliche Startschuss zur Verwirklichung des SEPA mit der Publikation der Verordnung über grenzüberschreitende Zahlungen im Dezember 2001;[28] diese verlangte die preisliche Gleichbehandlung von Inland- und Binnenmarktzahlungen, zudem forcierte sie die Umstellung auf IBAN und BIC.[29] Damit waren zwei Meilensteine auf dem Weg zu SEPA erreicht. Mit der ersten Zahlungsdiensterichtlinie vom November 2007 folgte der nächste Meilenstein.[30]

Die EU-Kommission zögerte sodann nicht, den Fahrplan für den SEPA-Prozess durch zusätzliches Verordnungsrecht auf Kurs zu halten. Vorgesehen war, dass die SEPA-Instrumente die nationalen Instrumente bis im Jahr 2010 ersetzen würden. Als sich herausstellte, dass dies nicht der Fall war, publizierte sie im März 2012 die SEPA-Migrationsverordnung.[31] Darin werden die Zahlungsdienstleister verpflichtet, die Eckpunkte von SEPA umzusetzen, namentlich die SEPA-Standards (IBAN) für Überweisungen und Lastschriften.

Das Eurosystem publiziert jährliche Fortschrittsberichte über den SEPA-Prozess. Die Fortschrittsberichte sind eng mit der EU-Kommission abgestimmt.[32] In den Berichten erfolgt eine Würdigung der bisherigen Umsetzung des SEPA, gleichzeitig werden aber auch die Erwartungen an die Zahl-

---

28 Verordnung (EG) Nr. 2560/2001 vom 19. Dezember 2001 über grenzüberschreitende Zahlungen in Euro (ABl Nr. L 344 v. 18.12.2001 S. 0013) (nicht mehr in Kraft). Zuvor schon: Mitteilung zum Massenzahlungsverkehr im Binnenmarkt, 31. Januar 2000, KOM (2000) 36 endg.

29 Siehe E. 11 und Art. 5, VO Nr. 2560/2001.

30 Die PSD1 ist schon von der Konzeption her keine reine SEPA-Richtlinie, sondern es geht bei der PSD1 um eine umfassende Regulierung des Zahlungsverkehrs. Aber die PSD1 ist z.B. relevant für SEPA, weil sie das Lastschriftenverfahren forciert hat.

31 Siehe die Erwägung Nr. 5 der Verordnung (EU) Nr. 260/2012 vom 14. März 2012 zur Festlegung der technischen Vorschriften […](ABl Nr. L 94 v. 30.03.2012, S. 22) («Die Selbstregulierung des europäischen Bankensektors im Rahmen der SEPA-Initiative hat sich als nicht ausreichend erwiesen …»).

32 Siehe etwa EZB, SEPA-Fortschrittsbericht 2006, S. 12 («Mit diesem Bericht, der mit der Europäischen Kommission abgestimmt ist, möchte das Eurosystem diese Unterstützung genauer und umfassender gestalten.»).

ungsdienstleister und insbesondere an den ECP hinsichtlich der weiteren Arbeiten formuliert.[33]

bb) Der European Payment Council

SEPA geht nicht ohne die Banken. Sie müssen letztlich die SEPA-Produkte bereitstellen. Das wichtigste koordinierende Beschlussorgan für das Bankgewerbe im Zusammenhang mit dem SEPA ist der European Payment Council, der 2002 gegründet wurde.[34] Seine Mitglieder sind Banken oder Branchenorganisationen der EU, des EWR und der Schweiz.[35] Die Anzahl der Sitze der einzelnen Länder ist abhängig von der Anzahl der Zahlungsverkehrstransaktionen in Euro des jeweiligen Landes und dessen Bevölkerung sowie einer angemessenen Repräsentanz aller Bankensektoren.[36]

Der ECP vertritt die Branche in den Diskussionen mit den EU-Organen, er entwickelt aber auch die verschiedenen technischen Standards und Instrumente zur Abwicklung der grenzüberschreitenden Zahlungen.[37] Von der Grundkonzeption her sollte die Kreditindustrie die Instrumente für ein paneuropäisches Zahlungssystem entwickeln, das – wegen seiner technischen Vorteile – die nationalen Zahlungssysteme ablösen würde. Der ECP sollte die Gesamtverantwortung für die Umsetzung des Migrationsprozesses übernehmen.[38] Es liegt auch in der Verantwortung des ECP, Kriterien festzulegen, anhand derer die SEPA-Konformität beurteilt werden kann.[39]

Man vertraute mit anderen Worten auf den Wettbewerb. Die EU-Kommission hat sich jedoch angesichts der Bedeutung von SEPA vorbehalten, die zu seiner Verwirklichung notwendigen Rechtsvorschriften vorzuschla-

---

33 Beispielhaft EZB, SEPA-Fortschrittsbericht 2006, S. 18: «Das Eurosystem erwartet, dass bis zum 1. Januar 2008 …[es folgt eine Liste mit Umsetzungsprojekten]»).

34 Zum ECP siehe HESS, Euro-Zahlungen, S. 62 f.

35 Schweizer Mitglied des ECP ist die UBS, siehe ECP-Website, Membership.

36 HESS/KEISER, SZW 2009, S. 158.

37 Z.B. bildet das einheitliche Datenformat für die Übermittlung von Zahlungsnachrichten (ISO 20022) die Grundlage für die Interoperabilität von Zahlungsverkehrsinfrastrukturen in SEPA und soll eine vollautomatisierte Abwicklung von Zahlungen ermöglichen. Erarbeitet wurde das Datenformat vom europäischen Kreditgewerbe, siehe HESS/KEISER, SZW 2009, S. 156. Für das Datenformat siehe SEPA Data Model, Version 2.2., approved on 13 December 2006 (EPC029-06).

38 EZB, SEPA-Fortschrittsbericht 2006, S. 13.

39 EZB, SEPA-Fortschrittsbericht 2006, S. 13.

gen oder einzuführen.[40] Das hat sie letztlich mit der SEPA-Migrationsverordnung dann auch getan.

Der ECP entwickelte in der Folge die Verfahren für die wesentlichen Zahlungsinstrumente: Die Buchgeldüberweisung (SEPA Credit Transfer), die Lastschrift (SEPA Direct Debit) und die Kartenzahlung (SEPA Cards Framework). Hinzu kommen das Verfahren für den SEPA Instant Credit Transfer und für den SEPA Direct Debit Business-to-Business. Die Datenformate von SEPA sind standardisiert, so dass eine vollautomatisierte Abwicklung möglich ist. Der ECP hat in Dokumenten die Funktionsweise der verschiedenen Zahlungsinstrumente (SEPA Schemes) festgelegt. Zentral sind dabei die sogenannten Regelwerke (Rule Books). Die Finanzdienstleister verpflichten sich vertraglich, die Regeln einzuhalten.[41] Der Beitritt zu den Schemes erfolgt über privatrechtliche Verträge, den sogenannten SEPA Adherence Agreements. Sie beinhalten die SEPA Rulebooks und die Pflicht, diese zu befolgen. Mit der Unterzeichnung der SEPA Adherence Agreements schliessen die teilnehmenden Finanzinstitute multilaterale Verträge mit dem European Payments Council und den anderen an SEPA teilnehmenden Finanzinstituten ab.[42] Vertragsparteien sind nicht Staaten, sondern die unterzeichnenden Finanzinstitute.

b) Teilnahme der Schweizer Finanzinstitute an den SEPA-Schemes

Die Schweiz wurde 2006 in den Kreis der SEPA-Mitgliedstaaten aufgenommen.[43] Die Teilnahmeberechtigung erlaubt es den Schweizer Instituten, die entsprechenden SEPA Adherence Agreements zu unterzeichnen.[44] Sie

---

40 Siehe EZB, Einheitliche Euro-Zahlungsverkehrsraum (SEPA), Pressemitteilung vom 4. Mai 2006, S. 2.

41 Für Einzelheiten zu den Inhalten siehe HESS, Euro-Zahlungen, S. 69 ff.

42 Siehe BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, Rn. C/18: Das Beitrittsabkommen untersteht belgischem Recht, für die einzelnen Vertragsverhältnisse gilt IPR, für die Kundenbeziehung gilt das nationale Recht (AGB). Siehe weiter HESS, Euro-Zahlungen, S. 73.

43 Siehe die Angaben auf der Webseite <www.sepa.ch>: Die Schweiz als Teil des Sepa-Raums.

44 Im November 2007 unterzeichneten die ersten Banken das SEPA Adherence Agreement (u.a. die UBS), ab Januar 2008 wurden erste SEPA-konforme Zahlungen

verpflichten sich damit gegenüber dem ECP und gegenüber den anderen teilnehmenden Finanzinstituten, die SEPA-Rulebooks zu befolgen.

Tatsächlich zeigt die Liste der teilnehmenden Institute, dass praktisch alle Schweizer Banken dem SEPA-Verfahren für Überweisungen beigetreten sind.[45] Für das Lastschriftenverfahren sind es lediglich deren dreizehn. Am B2B-Lastschriftenverfahren nehmen 10 Institute teil.[46] Das SEPA Instant Credit Transfer-Verfahren zeigt keine Schweizer Beteiligung. Die Ausführungen konzentrieren sich deshalb auf das SEPA-Überweisungsverfahren.

c) Teilnahmevoraussetzung: PSD-Äquivalenz

aa) PSD-Äquivalenz des allgemeinen Rechtsrahmens

Im SEPA-Projekt sind Regulierung und Selbstregulierung eng verzahnt. Grundlage für die SEPA-Regelwerke ist der gemeinsame Rechtsrahmen. Entsprechend stellt das SEPA-Rulebook für Überweisungen (Credit Transfer Scheme Rule Book, CTSR) in seinen Einleitungsartikeln klar, dass eine Teilnahme die Umsetzung der PSD (in ihrer geltenden Fassung) voraussetzt.[47] Für Finanzinstitute ausserhalb der EU musste diesbezüglich eine Lösung gefunden werden. Man hat sich für das Konzept der Äquivalenz entschieden, wobei davon nur die zivilrechtlichen Teile und nicht die aufsichtsrechtlichen

---

ausgeführt. Siehe dazu JURI, ClearIT 2007, S. 7. Zu den Teilnahmevoraussetzungen siehe Punkt c) Teilnahmevoraussetzungen.

45 Die teilnehmenden Banken können auf der ECP-Webseite (Register of Participants) eingesehen werden. <https://www.europeanpaymentscouncil.eu/what-we-do/participating-schemes/register-participants/registers-participants-sepa-payment-schemes>. Der Abgleich zwischen den von der FINMA bewilligten Banken und den am Credit Transfer Scheme beteiligten Banken (179) zeigt, dass die ausländisch beherrschten Banken das Adherence Agreement nicht unterzeichnet haben bzw. dass in diesen Fällen (wohl) die ausländische Mutterbank Teilnehmerin ist.

46 Besonders hervorzuheben ist die grosse Spannweite der teilnehmenden Institute. Neben den grossen Instituten wie Credit Suisse, UBS, Postfinance, Raiffeisen und den grossen ausländischen Banken JP Morgan Chase und BNP Paribas sind drei mittelgrosse Banken vertreten: Die Luzerner Kantonalbank, die Neue Aargauer Bank und die Bank CIC. Die zehnte Bank ist di Banca Popolare die Sondrio, eine Kleinbank.

47 Für die Teilnahme am Credit Transfer Scheme muss zusätzlich die Verordnung (EG) Nr. 1781/2006 vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers (ABl Nr. L 345 v. 8.12.2006, S. 1) betreffend Abgabe des Absenders eingehalten werden. Siehe dazu auch HESS/KEISER, SZW 2009, S. 150.

Teile der PSD betroffen sind. Verlangt wird mithin die Äquivalenz im Hinblick auf die Titel III und IV der PSD:

> «It is a prerequisite for the use of the Scheme that the Payment Services Directive *(or provisions or binding practice substantially equivalent to those set out in Title III and IV of the Payment Services Directive)* is implemented or otherwise in force in the national law of SEPA countries. »[48]

Die Schweizer Kreditinstitute mussten als Voraussetzung für ihren Beitritt nachweisen, dass in der Schweiz für den Bereich des Euro-Zahlungsverkehrs das Gesetz oder die Gerichtspraxis für die Rechtsbeziehung zwischen den Banken untereinander und den Banken und ihren Kundern einen Rechtsrahmen vorgeben, der mit den Regeln in der PSD im wesentlich gleichwertig ist. Die Finanzbranche hat ein solches Gutachten eingereicht, der ECP hat im September 2007 die Äquivalenz bejaht und gestützt darauf die Teilnahmemöglichkeit der Schweizer Finanzinstitute beschlossen.[49]

bb) PSD-Äquivalenz im Bank-Kundenverhältnis

Mit der abstrakten Äquivalenz des Rechtrahmens ist es aber für die Schweizer Kreditinstitute nicht getan. Weitergehend enthält das SEPA-Rulebook eine Sonderbestimmung für Banken aus Nicht-EU-Staaten mit dem Titel «Application of EU legislation between Participants». Danach verpflichten sich die Banken aus den Nicht-EU-Staaten gegenüber ihren Kunden zu einer Leistungserbringung, die als wesentlich gleichwertig mit der von der PSD geforderten Leistungserbringung anzusehen ist:

> «Each Participant that is not subject to the Payment Services directive under its national law shall vis-à-vis other Participants and *vis-à-vis its Customers* and to the the extent permitted by the national law applicable to such participant, comply with and perform obligations that are substantially equivalent to those provisions in Title III and IV of the Payment Services Directive which are relevant for SEPA Credit Transfers.» [50]

48 CTSR 2017, Art. 1.8.

49 HESS, Euro-Zahlungen, S. 75, Besprechung der relevanten Aspekte auf S. 76 ff.; HESS/KEISER, SZW 2009, S. 160.

50 CTSR 2017, Art. 5.14, erster Absatz.

Gemäss Rule Book sind zudem alle teilnehmenden Dienstleister verpflichtet, auf die Ausübung von national verankerten Rechten zu verzichten, sofern diese effektiv oder möglicherweise mit den Bestimmungen im Titel III und IV der PSD in Konflikt stehen könnten.[51] Anders gesagt: Rechspositionen, die sich aus dem nationalen Recht ergeben, sollen nur soweit ausgeschöpft werden, als sie sich innerhalb des SEPA-Rahmens bewegen.

Eine Ausnahme vom Äquivalenzerfordernis gilt im Hinblick auf diejenigen Bestimmungen in der PSD2, die sich mit den «Dritten Zahlungsdienstleistern» befassen. Dabei handelt es sich um Anbieter, die für ihre Dienstleistung einen direkten Zugriff auf die Konten ihrer Nutzer benötigen, ohne dass sie selbst diese Konten führen. Konkret handelt es sich um Drittemittenten von Zahlungskarten, Kontoinformationsdienste und Zahlungsauslösedienste.[52] Die PSD2 verpflichtet die Banken, mit den Dritten Zahlungsdienstleistern zu kooperieren, und gibt dem Bankkunden einen entsprechenden Anspruch. Im Gegenzug werden die Dritten Zahlungsdienstleister in das Pflichtenheft der PSD2 eingebunden und beaufsichtigt. Das Rule Book stellt diesbezüglich klar, dass der Kooperationszwang der Banken nur in Kombination mit einer Regulierung der Dritten Zahlungsdienstleister besteht. Soweit die Nicht-EU-Staaten ein solches Aufsichtsregimes nicht einführen, sind die Banken von einer zwangsweisen Öffnung ihrer Kontoinfrastruktur befreit.

Im Ergebnis ist festzuhalten, dass sich die Schweizer Banken gegenüber dem ECP und gegenüber den anderen SEPA-Teilnehmerbanken verpflichtet haben, im Euro-Überweisungsverkehr gegenüber ihren Kundinnen und Kunden die einschlägigen Vorgaben der PSD2 einzuhalten. Eine Ausnahme gilt für diejenigen Vorgaben, welche die Dritten Zahlungdienstleister betreffen.

---

51 CTSR 2017, Art. 5.14, zweiter Absatz: «Further, each Participant (whether or not subject to the Payment Services Directive) shall refrain, to the extent reasonably possible, form exercising any rights accorded to it under its national law vis-à-vis other Participants and vis-à-vis its Customers that either conflict or that could potentially conflict with the Provisions in Title III and IV of the Payment Services Directive.».

52 Für Einzelheiten siehe EMMENEGGER, Dritte Zahlungsdienstleister, S. 88 ff.

d) Rechtswirkung der SEPA-Teilnahme

Wenn sich die Banken zur Einhaltung der PSD2 im Falle von Euro-Überweisungen verpflichtet haben, so stellt sich die Frage, ob sich die Kundin in einer SEPA-relevanten Bankbeziehung auf eine der PSD festgelegten Pflichtenkatalog stützen kann. Im Vordergrund stehen der echte Vertrag zugunsten Dritter und der Vertrag mit Schutzwirkung zugunsten Dritter.

aa) Vertrag zugunsten Dritter

Ein direktes Forderungsrecht des Dritten auf eine versprochene Leistung kann gesetzlich, vertraglich oder gestützt auf eine Übung begründet werden.[53] Einschlägig für das direkte Forderungsrecht der Kunden im Rahmen der PSD ist die vertragliche Grundlage. Im Adherence Agreement verpflichtet sich die Bank (jede Bank) gegenüber ihren Vertragspartnern (die anderen teilnehmenden Banken und der EPC) zur Einhaltung des einschlägigen SEPA Rule-Books. Dort wiederum ist für Nicht-EU-Banken die Verpflichtung geregelt, gegenüber den Kunden die bankvertragsrechtlichen Regeln der PSD2 substantiell-äquivalent einzuhalten. Zwar enthalten weder das Adherence Agreement noch das Rule-Book eine ausdrückliche Klausel zum direkten Forderungsrecht des Kunden. Dieses ergibt sich aber aus dem Vertrauensprinzip:

SEPA ist ein EU-Projekt, an dem Banken aus wenigen Nicht-EU-Ländern teilnehmen können. Die privatrechtliche Verpflichtung der Nicht-EU-Banken zur Einhaltung der PSD2 soll den fehlenden Rechtsrahmen ersetzen, der für die EU-Banken zwingend gesetzt ist. Dieser Rechtsrahmen enthält in den einschlägigen Titeln III und IV der PSD2 flächendeckende, detaillierte und vor allem zwingende Vorgaben zum Zivilrecht des Zahlungsverkehrs. Innerhalb der EU ist völlig klar, dass die dort geregelten Ansprüche von den Kunden zivilrechtlich durchgesetzt werden können. Das PSD2-Privatrecht findet sich nicht nur als zwingendes Privatrecht in den Zivilgesetzbüchern,[54] sondern es findet sich in wörtlicher Widergabe in den AGB der europäischen Banken zum Zahlungsverkehr. Das ist kein Zufall: Die PSD2 schreibt

---

53 Siehe dazu im Einzelnen KRAUSKOPF, Der Vertrag zugunsten Dritter, S. 224 ff., 228 ff., 242 ff. und 248 f.

54 Beispielhaft: §§ 375c – 376c BGB.

in Titel III den Banken vor, über welche Punkte sie die Kundinnen und Kunden im Hinblick auf ihre Zahlungsdienstleistung informieren müssen. Im EU-Raum führt das zu harmonisierten AGB im Zahlungsverkehr. Wenn die Schweizer Banken den EU-Banken und dem European Payments Council zusichern, dass sie im Bank/Kunden-Verhältnis das PSD-Privatrecht substantiell-äquivalent einhalten, so können ihre SEPA-Vertragspartner diese Zusicherung nach Treu und Glauben nur dahingehend verstehen, dass den Kunden der Schweizer Banken die wesentlich gleichen Ansprüche zustehen, die auch im EU-Raum gelten, und zwar als direkter Anspruch gegenüber den Banken. Dies nicht zuletzt auch deshalb, weil das Prinzip der gleichen Wettbewerbsbedingungen zu den tragenden Säulen des SEPA-Agreements gehört.[55] Insgesamt ergibt also die Auslegung von Rule 5.14 des SEPA Rulebooks anhand des Vertrauensprinzips, dass in der dort festgelegten Verpflichtung zur Einhaltung des PSD2-Privatrechts eine echte Vereinbarung zugunsten Dritter (Art. 112 OR) zu sehen ist. Entsprechend sind die Kunden im Falle von Euro-Überweisungen berechtigt, von der Bank die (substantiell äquivalente) Einhaltung des PSD2-Privatrechts zu verlangen.

Gegen dieses Resultat lässt sich auch nicht einwenden, dass die PSD2 eine Richtlinie ist und somit von den Mitgliedstaaten zunächst einmal in rechtlich einforderbare Regeln umgesetzt werden muss. Wie bereits ausgeführt wurde, operiert die PSD2 auf der Grundlage der Vollharmonisierung[56] und sie statuiert sehr konkrete und genaue Pflichten. Entsprechend übernehmen die nationalen Umsetzungsgesetze die Richtlinie praktisch wörtlich und auch die AGB der EU-Banken enthalten praktisch wörtliche Wiedergaben der PSD2-Pflichten für den Zahlungsdienstevertrag. Insofern steht einer direkten Anwendbarkeit der PSD2-Pflichten nichts entgegen. Hinzu kommt, dass es Vertragsparteien freisteht, die Einhaltung von jedwelchen Pflichten zu statuieren. Einigen sie sich auf die Einhaltung der Pflichten gemäss PSD2, so sind diese Pflichten für die Parteien verbindlich. Soweit sich ein Auslegungsbedarf ergibt, ist das Vertrauensprinzip heranzuziehen.

---

55 Siehe dazu Rule 5.1 CTSR 2017, erstes Lemma.

56 Siehe Art. 107 Abs. 2 PSD2. Zur Regeldichte siehe auch GRUNDMANN, WM 2009, S. 1110, der die Regelung als «flächendeckend» im Bank-Kunden-Verhältnis bezeichnet.

Nicht stichhaltig wäre schliesslich der Einwand, es bestehe für die Schweizer Banken als Nicht-EU-Mitgliedsbanken gemäss Rule 5.14 CTSR nur eine Pflicht zur im Wesentlichen gleichwertigen (substantially equivalent) Umsetzung der PSD2-Pflichten im Zahlungsdienstevertrag. Das ist richtig; es bedeutet, dass man die PSD2-Pflichten nicht auf jeden Punkt und jedes Komma umsetzen muss. Es bedeutet aber, dass man ein gleichwertiges Schutzniveau einhalten muss. Unterschreitet man erkennbar das Schutzniveau, liegt eine Pflichtverletzung vor. Ob eine solche Unterschreitung vorliegt, lässt sich anhand der AGB-Regelungen der Schweizer Banken relativ einfach feststellen.

Im Ergebnis liegt in der Zusicherung der Schweizer Banken, bei Euro-Überweisungen die Bestimmungen der PSD2 in der Bank-Kundenbeziehung substantiell-äquivalent umzusetzen, ein echter Vertrag zugunsten Dritter (Art. 112 OR). Der Kunde kann also von der Bank eine PSD2-konforme Ausgestaltung der Vertragsbeziehung verlangen und er kann sich in einer allfälligen Auseinandersetzung der Bank auf seine Rechte gemäss PSD2 berufen.

bb) Vertrag mit Schutzwirkung zugunsten Dritter

Eine weitere Grundlage für direkte Ansprüche der Kunden von Schweizer Banken liegt in der Rechtsfigur des Vertrags mit Schutzwirkung zugunsten Dritter. Bei diesem steht – im Unterschied zum echten Vertrag zugunsten Dritter – die Hauptleistung allein dem Gläubiger zu. Der Dritte ist aber insofern in die vertraglichen Schutz- und Sorgfaltspflichten eingebunden, als er bei deren Verletzung Schadenersatzansprüche geltend machen kann.[57] Der Vertrag mit Schutzwirkung zugunsten Dritter dient in diesem Sinne als Auffangordnung für Schadenersatzklagen, wenn man das Vorliegen eines echten Vertrages zugunsten Dritter verneint.

Der Vertrag mit Schutzwirkung zugunsten Dritter ist im Obligationenrecht nicht ausdrücklich geregelt. Er wird aber als Rechtsfigur von der Lehre ganz überwiegend anerkannt.[58] Das Bundesgericht hat in mehreren Ent-

[57] Siehe etwa GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT II, Rn. 3913.

[58] Siehe die Nachweise bei GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT II, Rn. 3913 und sodann FOUNTOULAKIS, AJP 2018, S. 97.

scheiden die Anwendungsvoraussetzungen des Vertrages mit Schutzwirkung zugunsten Dritter geprüft. Es ist aber jeweils zum Schluss gekommen, die Voraussetzungen seien im konkreten Fall nicht erfüllt.[59] Es gibt also noch keinen *Leading Case.* Der Vertrag über die SEPA-Teilnahme weist indessen alle Ingredienzen auf, um – *when tested in court* – zu einem erfolgreichen Grundsatzentscheid zu avancieren.

Die Anwendungsvoraussetzungen können mit folgenden Stichworten umschrieben werden: Leistungsnähe, Schutzinteresse, Erkennbarkeit:[60]

– Das Kriterium der Leistungsnähe erfordert, dass der *Dritte bestimmungsgemäss mit der Haupleistung des Vertrages in Berührung kommt*. Das ist im Fall des SEPA Adherence Agreements für Überweisungen (der für den konkreten Pflichteninhalt auf das Rule Book verweist) zweifellos der Fall: Die Banken verpflichten sich gegenseitig und gegenüber dem ECP zu Verhaltenspflichten gegenüber Kunden im Überweisungsverkehr. Der Kunde kommt mit diesen Verhaltenspflichten im Rahmen seines Überweisungsauftrags an die Bank unmittelbar in Berührung.

– Das Kriterum des Schutzinteresses erfordert, dass die Gläubigerin der Hauptleistungspflicht ein *schutzwürdiges Interesse an der Einbeziehung des Dritten in die vertragliche Sorgfaltspflicht* hat. Auch dies ist im Falle des SEPA Adherence Agreements gegeben: Wenn die Banken sich im Rule Book ausdrücklich zur Einhaltung des PSD2-Privatrechts und der dort geregelten Pflichten gegenüber den Kunden verpflichten,[61] so haben sie

---

59 In BGE 130 III 345 E. 1 S. 348 hat es zudem ausgeführt, es habe die Rechtsfigur des Vertrags mit Schutzwirkung zugunsten Dritten noch nie grundsätzlich bejaht. Der spätere BGer 4A_226/2010 E. 3.2.1 verzichtet beim Verweis auf BGE 130 III 345 auf diese Formulierung und hält lediglich fest, die Anwendungsvoraussetzungen seien bislang nicht erfüllt gewesen.

60 Siehe BGer 4C.194/1999 E. 4: Voraussetzung, wonach «le *tiers soit touché*, ou concerné, par l'execution de la prestation principale, que *le créancier* de celleci ait *avantage à l'inclusion du tiers* dans les intérêts contractuellement protégés, et que le *débiteur puisse reconnaître* cela.» Siehe auch die Nachweise bei GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT II, Rn. 3913. Die Kriterien entsprechend den anerkannten Anwendungsvoraussetzungen in der deutschen Lehre und Rechtsprechung, siehe zuletzt BGH, Urteil vom 07.12.2017 – VII ZR 204/14.

61 Das Rule Book führt zudem weitergehend aus, dass die Vertragsparteien – unabhängig von ihrer Unterstellung unter die PSD2 – von der Ausübung von Rechten untereinander *und gegenüber den Kunden*, die ihnen kraft nationalen Rechts zustehen,

ein offensichtliches und schutzwürdiges Interesse daran, dass diese Pflichten gegenüber den Kunden auch effektiv eingehalten werden. Die Kunden sind explizit Gegenstand der vereinbarten Sorgfaltspflichten. Also sind sie notwendigerweise in diese Verpflichtungen eingebunden. Hier zeigen sich auch grundlegende Unterschiede zu den bisherigen Fällen, die dem Bundesgericht vorgelegen haben, insbesondere der Fällen der Gutachterhaftung bei Liegenschaftsschätzungen.[62] Im Liegenschafts-Entscheid wurde das Gutachten explizit für einen Kunden (Hauseigentümer) und für einen bestimmten Zweck (Liegenschaftsschätzung für Versicherungspolice) erstellt. Deshalb durfte sich der Dritte (Hauskäufer) nicht auf das Gutachten berufen, denn der Gutachter hatte sich nicht zur Erstellung eines Gutachtens für einen Hausverkauf verpflichtet und die potentiellen Käufer waren nicht Gegenstand seiner Sorgfaltspflichten.

Schliesslich ergibt sich das schutzwürdige Interesse an der Einbeziehung der Kunden in die vertraglich vereinbarten Sorfaltspflichten daraus, dass die Beteiligung am SEPA-Mechanismus auf der Grundlage beruht, dass für alle dieselben Wettbewerbsbedingungen gelten und dass alle Beteiligten sich in gleicher Weise an das Rule Book halten.[63] Der Grundsatz der gleichen Wettbewerbsbedingungen führt dazu, dass alle ein schutzwürdiges Interesse daran haben, dass für alle derselbe Pflichtenkatalog und die gleichen (direkten) Durchsetzungsmöglichkeiten gelten.

– Das Kriterium der Erkennbarkeit besteht darin, dass das *Drittschutzinteresse für die haftende Vertragspartei erkennbar* gewesen sein muss. Auch dieses Kriterium ist im Fall des Adherence Agreements erfüllt. Wenn die Vertragsparteien sich gegenseitig verpflichten, gegenüber den Kunden

soweit zumutbar absehen, sofern diese effektiv oder möglicherweise mit den Bestimmungen im Titel III und IV der PSD in Konflikt stehen könnten. Siehe CTSR 2017, Art. 5.14, zweiter Absatz oben Fn. 51.

62 BGE 130 III 345 E. 1 S. 348.

63 SEPA Instant Credit Transfer Scheme Rulebook, Version 1.1., approved on 18 October 2017 (EPC 004-16), Rule 5.1. (Participation in the SEPA Credit Transfer Scheme is on the basis of compliance with the following principles: Scheme Participants from all countries in SEPA participate on the basis that the level playing field is respected. All adhering Scheme Participants shall comply with the SEPA Credit Transfer Scheme Rulebook on the same basis as other Participands.

gewisse Verhaltenspflichten einzuhalten, dann ist für sie das Interesse der Kunden an dieser Einhaltung ohne Weiteres erkennbar.

Als Fazit lässt sich Folgendes festhalten: Selbst wenn man davon ausgehen würde, dass das SEPA Adherence Agreement keinen echten Vertrag zugunsten der Schweizer Bankkunden bei SEPA-Überweisungen beinhaltet, so besteht ein Auffangtatbestand mit dem Vertrag mit Schutzwirkung zugunsten Dritter. Denn in der Verpflichtung der Schweizer Banken zur Einhaltung der Verhaltenspflichten im Bank/Kundenverhältnis im Rahmen des SEPA Adherence Agreements liegt eine solche Schutzwirkung. Erleidet der Kunde einen Schaden, weil die Bank ihre Pflichten gemäss PSD2 verletzt hat, so kann er diesen geltend machen. Im Hinblick auf mögliche Einwände bezogen auf den Richtliniencharakter der PSD2 und die substantielle Äquivalenz (im Gegensatz zur wörtlichen Übernahme) kann auf die Ausführungen im Zusammenhang mit dem Vertrag zugunsten Dritter verwiesen werden.

III. Struktur der PSD2

Die PSD2 umfasst 93 Seiten, fünf Titel und 117 Artikel. Sie wird eingeleitet durch 113 Erwägungen des Europäischen Parlaments und des Rats der Europäischen Union. Wie ihre Vorgängerversion operiert die PSD2 auf der Grundlage der Vollharmonisierung.[64] Sie ist zudem – wie praktisch alle Rechtsakte der EU – als Einheitsgesetz konzipiert: Sie enthält also einen aufsichtsrechtlichen (Titel II) und einen zivilrechtlichen Teil (Titel III und IV).[65] Hervorzuheben ist beim zivilrechtlichen Teil, dass die PSD2 darin mit

64 Art. 107 Abs. 1 PSD2; Art. 86 PSD1.

65 Siehe dazu und zur Umsetzung im deutschen Recht durch das ZAG (Aufsichtsrecht) und das BGB, EGBG und UklaG (Zivilrecht): BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte Rn. C/2 ff. Hilfreich insb. auch die in Rn. C/5 enthaltene Konkordanztabelle zur PSD2 und den BGB-Bestimmungen. Zu den Schwierigkeiten einer einwandfreien Zuweisung zu den Rechtsgebieten und ingesamt zur (gespaltenen) Umsetzung siehe OMLOR, WM 2018, S. 57 ff.

beachtlicher Detaildichte einen neuen Nominatvertrag gestalten, nämlich den Zahlungsdienstevertrag.[66]

1. Titel I: Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Titel I (Art. 1-4) regelt den *Gegenstand, Anwendungsbereich und die Begriffsbestimmungen* der Richtlinie. Hier wird unter anderem festgehalten, dass die Richtlinie für alle Zahlungsdienste gilt, die innerhalb der Union erbracht werden. Die zivilrechtlichen Teil (Titel III und IV) sind anwendbar, wenn die Dienstleister in der Union ansässig sind (Art. 2 Abs. 2). Sie finden darüber hinaus (mit Ausnahmen) Anwendung, wenn eine Drittwährung verwendet wird, solange ein beteiligter Dienstleister in der Union ansässig ist (Art. 2 Abs. 3 und 4). Auf diese «One-Leg-Transactions» gilt die Richtlinie allerdings nur für die in der Union getätigten Bestandteile des Zahlungsvorgangs.[67]

2. Titel II: Zahlungsdienstleister

Titel II (Art. 5-37) befasst sich mit den *Zahlungsdienstleistern* und regelt die wesentlichen aufsichtsrechtlichen Fragen. Sie betreffen das Zulassungsverfahren, die Zulassungsvoraussetzungen und die laufende Überwachung einschliesslich des Zulassungsentzugs (Art. 5 - Art. 18).[68] Die Regelungen sind von ihrem Inhalt her ähnlich gestaltet wie die Bewilligungsverfahren für die Zulassung von Finanzinstituten nach BankG, allerdings angepasst auf die Breite möglicher Zahlungsdienste und die entsprechende Vielfalt der Marktakteure.[69] Aus der Unionsperspektive stechen zudem die Einschränkungen im Hinblick auf die Freizügigkeit (single passport) hervor. So wurde die Stellung der Behörden des Aufnahmestaates im Hinblick auf eine mögliche Ablehnung der Niederlassung gestärkt (Art. 28). Auch bestehen

66 So schon zur PSD1, siehe dazu GRUNDMANN, WM 2009, S. 1110 ff. Im deutschen BGB findet sich der Zahlungsdienstevertrag im Wesentlichen in § 675c - 676c BGB.

67 Siehe hierzu auch OMLOR, ZIP 12/2016, S. 560; TERLAU, ZBB 2016, S. 125.

68 Für einen Überblick siehe TERLAU, ZBB 2016, S. 128 ff.

69 Beispielsweise beträgt das Mindest-Anfangskapital für Zahlungsauslösedienste € 50'000.-- (Art. 7 lit. b i.V.m. Anhang I Nr. 7 PSD2).

Berichtspflichten des ausländischen Zahlungsinstituts an die Behörde des Aufnahmestaates, und diese ist auch zur Überwachung der zivilrechtlichen Vorschriften durch das ausländische Zahlungsinstitut befugt (Art. 29 Abs. 2). Anlass dazu gaben offenbar die zahlreichen Fälle regelwidriger Tätigkeiten von Agenten oder Zweigniederlassungen von Instituten mit Sitz in einem anderen Mitgliedstaat.[70]

3. Titel III: Transparenz der Vertragsbedingungen und Informationspflichten

Titel III (Art. 38-60) enthält den ersten zivilrechtlichen Teil der Richtlinie. Er trägt den Titel *Transparenz der Vertragsbedingungen und Informationspflichten der Zahlungsdienste.* Darin schreibt die Richtinie im Ergebnis vor, welche Inhalte in den AGB der Zahlungdienstleister enthalten sein müssen.[71] Die Inhaltsvorgaben selbst sind zu wesentlichen Teilen in Titel IV geregelt. Vereinzelt enthält Titel III aber auch inhaltliche Pflichten für Zahlungsdienste und ihre Nutzer, etwa die Regeln zur Vertragsänderung und zur Kündigung des Rahmenvertrags (Art. 54, 55).

4. Titel IV: Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten

Titel IV (Art. 61-103) enthält den zweiten zivilrechtlichen Teil der Richtlinie. Er konkretisiert die *Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten.* Hier wird der Zahlungsdienstevertrag inhaltlich abgesteckt. Entsprechend umfangreich gestaltet sich in diesem Teil auch die Richtlinie. Im ersten Kapitel geht es um die verschiedenen Aspekte des Entgelts für die Erbringung von Zahlungsdienstleistungen (Art. 62, 63). Das zweite Kapitel regelt die Rahmenbedingungen für die Autorisierung von Zahlungsvorgängen (Art. 64, 65), den Kontozugang von und die Verpflichtungen seitens dritter Zahlungsdienstleister (Art. 66, 67), die Sorgfaltspflichten im Hinblick auf die Zahlungsinstrumente (Art. 69, 70), das Verfahren

70 So TERLAU, ZBB 2016, S. 129.

71 Für die Umsetzung im deutschen Recht siehe § 675d BGB und Artikel 248 §§ 1 ff. EGBGB.

und die Haftung bei unautorisierten Zahlungsvorgängen (Art. 71-75) und die Erstattungspflichten im Lastschriftenverfahren (Art. 76, 77). Das dritte Kapitel befasst sich mit der Ausführung von Zahlungsvorgängen und statuiert unter anderem die Unwiderruflichkeit von Zahlungsaufträgen, die Verpflichtung zum Transfer des vollen Betrages, die Ausführungsfristen und Wertstellungsdaten (Art. 82-87) und schliesslich die Haftung bei fehlerhaften Kundenidentifikatoren und bei nicht erfolgter, fehlerhafter oder verspäteter Ausführung von Kundenaufträgen (Art. 88-91). Das vierte Kapitel regelt den Datenschutz (Art. 94). Das fünfte Kapitel befasst sich mit den operationellen und sicherheitsrelevanten Risiken und der Authentifizierung. So sind die Zahlungsdienstleister für angemessene Sicherheitsmassnahmen verantwortlich.[72] Geregelt ist auch die starke Kundenauthentifizierung (Art. 97, 98). Darüberhinaus werden hier Meldepflichten bei schwerwiegenden Betriebs- oder Sicherheitsvorfällen festgelegt, einschliesslich einer Meldepflicht gegenüber dem Nutzer, sofern sich der Vorfall auf die finanziellen Interessen des Nutzers auswirkt oder auswirken könnte.[73] Das abschliessende sechste Kapitel regelt die verschiedenen Rechtsbehelfe im Zusammenhang mit Zahlungsdienstleistungen (Art. 99-103). So können beispielswese Zahlungsdienstnutzer und andere interessierte Parteien (einschlisslich Verbraucherverbänden) bei den zuständigen Behörden Beschwerde wegen mutmasslicher Verstösse der Zahlungsdienstleister gegen diese Richtline einlegen. Damit werden die Aufsichtsbehörden in die Einhaltung der zivilrechtlichen Bestimmungen der Richtlinie eingebunden. Auch werden die Banken durch die PSD2 verpflichtet, Kundenbeschwerden innerhalb von 15 Arbeitstagen zu beantworten.[74] Sie informieren die Kunden auch über mindestens eine Stelle zur alternativen Streitbeilegung.[75]

72 Art. 95 PSD2.
73 Art. 96 Abs. 1 PSD2.
74 Art. 101 PSD2.
75 Art. 101 Abs. 3 PSD2.

5. Titel V: Delegierte Rechtsakte und Technische Regulierungsstandards

Titel V (Art. 104-106) trägt den Titel *Delegierte Rechtsakte und Technische Regulierungsstandards.* Er regelt die Befugnis der Kommission, bestimmte Anpassungen der Richtlinie vorzunehmen, beispielsweise die Anpassung des Höchstbetrages der Haftung des Kunden bei unautorisierten Transaktionen (Art. 73 Abs. 1), sodann verpflichtet er die Kommission zur Erstellung eines benutzerfreundlichen elektronischen Merkblatts über die Rechte der Verbraucher gemäss der PSD2.

6. Titel VI: Schlussbestimmungen

Titel VI enthält die *Schlussbestimmungen.* Er bestimmt unter anderem, dass die Umsetzung der Richtlinie in nationales Recht bis am 13. Januar 2018 zu erfolgen hat, wobei die Sicherheitsmassnahmen 18 Monate nach dem Inkrafttreten der Regulierungsstandards anzuwenden sind.

IV. Ausgewählte Eckpunkte in Titel III der PSD2

1. Generelle Informationspflichten und Vertragsbedingungen

a) Regelung in der PSD2

Während Titel IV der PSD2 die Rechte und Pflichten des Zahlungsdienstevertrags festlegt, stellen die Informationspflichten des Titels III sicher, dass diese in den (allgemeinen) Vertragsbedingungen des Zahlungsdienstes auch effektiv so festgehalten werden. Die Richtlinie unterscheidet zwischen Einzelzahlungen und Zahlungen im Kontext von Rahmenverträgen.[76] In beiden Fällen bestehen generelle Informationspflichten.[77] Es handelt sich erstens um Informationen hinsichtlich der *Dienstleistung*, etwa notwendige Zahlungsinformationen[78], die maximale Ausführungsfrist,[79] die Entgelte und deren

[76] Art. 43 ff. (Einzelzahlungen), Art. 50 ff. (Rahmenverträge).

[77] Art. 45, 52 PSD2. Diese Informationen müssen vorgängig zugänglich sein: Art. 44, 51 PSD2.

[78] Art. 45 Abs. 1 lit. a, Art. 52 Ziff. 1 lit. b PSD2.

Aufschlüsselung,[80] allfällige Wechselkurse.[81] Zweitens werden Informationspflichten mit Bezug auf den *Zahlungsauftrag bzw. Zahlungsausführung* statuiert, z.B. die Transaktionsreferenz, den Betrag der Belastung bzw. der Gutschrift, die Entgelte, den allfälligen Wechselkurs und das Wertstellungsdatum der Belastung bzw. der Gutschrift.[82]

Weitere Informationspflichten betreffen die Schutz- und Abhilfemassnahmen, unter anderem Vorkehrungen zur sicheren Aufbewahrung von Zahlungsinstrumenten, die Anzeigepflichten bei Verlust, Diebstahl etc., die Risikoverteilung bei unautorisierten Zahlungen und die Haftung bei fehlerhafter Ausführung.[83] Informiert werden muss sodann über die Möglichkeiten eines Beschwerdeverfahrens und die zuständigen Behörden.[84]

Gewisse Informationspflichten sind für die Schweizer Banken im Zusammenhang mit dem hier interessierenden SEPA-Überweisungssystem nicht relevant. Das gilt für die Informationspflichten im Lastschriftenverfahren,[85] die eben nur für diejenigen Banken beachtlich sind, die dem SEPA-Lastschriften-Scheme beigetreten sind. Auch die Informationspflichten, welche die Drittzahlungsdienstleister, namentlich die Zahlungsauslösedienste betreffen,[86] sind nicht von der Äquivalenzverpflichtung erfasst; das SEPA-Rulebook stellt in Rule 5.1 klar, dass die diesbezüglichen Bestimmungen aufgrund der fehlenden Aufsicht über die Drittzahlungsdienstleister in den Nicht-EU-Staaten nicht zur Anwendung kommen.

79 Art. 45 Abs. 1 lit. b, Art. 52 Ziff. 2 lit. e PSD2.

80 Art. 45 Abs. 1 lit. c, Art. 52 Ziff. 2 Ziff. 3 PSD2.

81 Art. 45 Abs. 1 lit. d, Art. 52 Ziff. 2 Ziff. 3 PSD2.

82 Art. 48 lit. a-e (Zahler, Einzelzahlung, nach Eingang Zahlungsauftrag), Art. 49 lit. a-e (Zahlungsempfänger, Einzelzahlung, nach Ausführung Zahlungsvorgang); Art. 57 lit. a-e (Zahler, Rahmenvertrag, nach Kontobelastung), Art. 58 lit. a-e PSD2 (Zahlungsempfänger, Rahmenvertrag, nach Ausführung Zahlungsvorgang).

83 Art. 45 Abs. 3 i.V.m. Art. 52 Ziff. 5 PSD2 (für Einzelzahlungen), Art. 52 Ziff. 5 PSD2 (für Rahmenverträge).

84 Art. 52 Ziff. 7 lit. b PSD2.

85 Art. 52 Ziff. 5 lit. g PSD2 unter Hinweis auf Art. 76 und 77 PSD2.

86 Art. 45 Abs. 2 lit. a und b, Art. 46, Art. 47 PSD2.

b) Regelung in den AGB der Schweizer Banken

Die AGB-Praxis der Banken nimmt nicht deckungsgleich alle Punkte auf, über die in Titel III eine Information gefordert wird. Gewisse Punkte fehlen sodann, weil es in der Schweiz keine entsprechenden Verfahren gibt, etwa das in der PSD2 vorgesehene Beschwerdeverfahren. Zahlreiche Punkte sind aber standardmässig enthalten, so etwa die Informationen über die Dienstleistung, die Informationen über den Zahlungsauftrag und die Zahlungsausführung, und die Haftung bei unautorisierten Transaktionen.

c) Fazit

Hinsichtlich der Informationen, welche in den AGB zum Zahlungsverkehr enthalten sind, gibt es weitgehende Überschneidungen mit den Vorgaben der PSD2, auch wenn die Detailldichte teilweise geringer ist. In der Gesamtschau kann man von einem äquivalenten Informationsniveau sprechen.[87] Wenn sich die Zahlungsverkehrs-AGB der Schweizer Banken von den entsprechenden AGB der EU-Banken unterscheiden, so liegt es in erster Linie am *Inhalt* der Regelungen und nicht an der Liste der Regelungspunkte.

2. Kontorelevante Bestimmungen

a) Regelung in der PSD2

Im Zusammenhang mit den Rahmenverträgen enthält Titel III auch inhaltliche Vorgaben zum Kontovertrag.[88] So darf etwa bei Zahlungskonten für die monatliche Kontoübersicht keine Gebühr verlangt werden.[89] Geregelt werden auch die Änderungen der zahlungsrelevanten Vertragsbedingungen.[90] Sie müssen zwei Monate vor Inkrafttreten angezeigt werden,[91] wobei

87 So auch HESS, Euro-Zahlungen, S. 80.

88 So auch GRUNDMANN, WM 2009, S. 1113 (zur diesbezüglich gleich aufgebauten PSD1).

89 Art. 57 Abs. 2 PSD2. Gemäss Art. 57 Abs. 3 PSD2 können die Mitgliedstaaten als weitergehende Regelung verlangen, dass die Information in Papierform oder auf einem anderen dauerhaften Datenträger mindestens einmal monatlich kostenlos mitgeteilt wird.

90 Art. 54 PSD2.

91 Art. 54 Abs. 1 PSD2.

die Banken eine Genehmigungsfiktion vorsehen können, falls der Kunde die Ablehnung nicht vor dem vorgeschlagenen Tag des Inkrafttretens der Änderung angezeigt hat.[92] Im Falle der Ablehnung der Änderungen hat der Kunde das Recht, den Rahmenvertrag jederzeit bis zum Tag der Anwendung der Änderungen kostenlos zu kündigen.[93]

Geregelt wird in Titel III auch die Kündigung des Zahlungsdienst-Rahmenvertrags – und damit des Zahlungskontovertrags. Der Kunde kann den Vertrag jederzeit und kostenlos[94] kündigen, wobei die Vereinbarung einer Höchstkündigungsfrist von einem Monat zulässig ist. Das Kündigungsrecht der Bank bedarf demgegenüber der besonderen Regelung (wobei eine AGB-Regelung zulässig ist). Sie beträgt zwei Monate.[95] In der (deutschen) Lehre wird darauf hingewiesen, dass eine Kündigung aus wichtigem Grund möglich bleibt.[96]

b) Regelung in den AGB der Schweizer Banken

In der Schweiz sind Gebühren für die Führung eines Zahlungskontos durchaus üblich. Sie beziehen sich aber nicht spezifisch auf die Zusendung der Kontoübersicht, weshalb die Praxis den Vorgaben der PSD2 jedenfalls formell entspricht.

Vertragsänderungen sind in den AGB durchweg über die Genehmigungsfiktion geregelt, was die PSD2 auch ausdrücklich vorsieht. Hingegen fehlt jeweils eine Bestimmung über die zweimonatige Ankündigungsfrist – was Folgen hat für die weitere Regelung der Zustimmung bzw. Ablehnung der Änderung. Ohne einen festen Zeitpunkt für die Vertragsänderung mit (mindestens) zweimonatiger vorheriger Ankündigungsfrist ist es nicht möglich, dem Kunden bis zu dieser Änderung ein Widerspruchsrecht einzuräumen. Stattdessen wird dem Kunden meist eine 30-tägige Widerspruchsfrist

92 Art. 54 Abs. 1 PSD2 Unterabsatz 2.

93 Art. 54 Abs. 1 PSD2 Unterabsatz 2.

94 Eine Ausnahme von der Kostenlosigkeit gilt für Verträge, die weniger als sechs Monate in Kraft waren (Art. 55 Abs. 2 PSD2).

95 Art. 55 Abs. 3 PSD2.

96 GRUNDMANN, WM 2009, S. 1114. Der Autor weist zudem darauf hin, dass im Falle einer fehlenden Kündigungsabrede ein ewiger Vertrag nach deutschem Recht sittenwidrig wäre. Allerdings ist nicht anzunehmen, dass die Banken eine Kündigungsklausel weglassen.

eingeräumt, nach deren Ablauf die Genehmigungsfiktion greift. Das ist allerdings nur halb so lang wie die Frist in der PSD2. Darüber hinaus sehen gewisse AGB vor, dass die erste Nutzung seit Bekanntgabe der Änderung als Genehmigung gilt. Das widerspricht nicht nur der PSD2, sondern es verstösst auch gegen Art. 8 UWG. Denn jedenfalls im E-Banking – und dieses bildet in der Schweiz den Standardfall – wird der Kunde über die Änderung informiert, wenn er eine Zahlung auslösen will. In diesem Moment ist er aber in seiner Entscheidungsfreiheit massiv beeinträchtigt, denn er will die geplante Zahlung fristgerecht auslösen, und nicht zuerst bei einer anderen Bank ein Konto eröffnen, um dann die Zahlung vorzunehmen. Ihm aufgrund der Nutzung des Zahlungsdienstes eine Zustimmung zu unterstellen, ist treuwidrig.

Unterschiedlich geregelt sind schliesslich die Kündigungsfristen. Die AGB der Schweizer Banken sehen ein jederzeitiges, beidseitiges Kündigungsrecht vor. Es gibt also keine einmonatige Höchstfrist für den Kunden und es gibt auch keine zweimonatige Mindestfrist für die Banken. Beides wäre ein Verstoss gegen das zwingende sofortige Kündigungsrecht in Art. 404 Abs. 1 OR. Soweit die Kundenseite betroffen ist, kann man den Widerspruch auflösen, denn die PSD2 sieht vor, dass die Mitgliedstaaten Vorschriften erlassen können, die für den Zahlungsdienstnutzer vorteilhafter sind.[97] Damit bleibt es beim Unterschied hinsichtlich der zweimonatigen Mindestfrist für die bankseitige Kündigung, die in den AGB der Schweizer Banken nicht abgebildet ist und nach schweizerischem Recht auch nicht zulässig wäre.

c) Fazit

Während die AGB-Praxis der Schweizer Banken hinsichtlich der Informationspflichten zum Überweisungsverkehr im Grossen und Ganzen den Vorgaben der PSD2 entspricht, zeigen sich bei den kontorelevanten Bestimmungen des dritten Titels der PSD2 deutliche Unterschiede.

Allerdings stellt sich die Frage, ob sich die Schweizer Banken überhaupt zur Einhaltung dieser Vorgaben verpflichtet haben. Denn das Rule Book verlangt die Einhaltung der Vorgaben der PSD (Titel III und IV) nur inso-

[97] Art. 55 Abs. 6 PSD2.

fern, als sie «relevant für SEPA Credit Transfers» sind – also nur für Euro-Überweisungen.[98] Die Verpflichtung betrifft also die *transaktionsbezogenen* Bestimmungen in Titel III und IV, und nicht diejenigen, die sich auf die Kontoführung beziehen. Dafür sprechen auch der Gegenstand und die Zielsetzung des SEPA-Regelwerks für den Überweisungsverkehr. Das Regelwerk (Scheme) soll Euro-Überweisungsverkehr regeln (Rule 1.1., Vision) und es soll die Unterschiede zwischen nationalen und grenzüberschreitenden Zahlungen eliminieren. Das Regelwerk, dem die Schweizer Banken beigetreten sind, fokussiert also auf die Transaktion und nicht auf die Kontoführung. Die beiden Bereiche sind zwangsläufig eng verknüpft und für die Teilnehmenden aus den EU-Mitgliedstaaten spielt die Unterscheidung auch keine Rolle. Für die teilnehmenden Kreditinstitute aus Nicht-EU-Ländern ist diese Einschränkung aber von Bedeutung.

Allerdings ist zu beachten, dass selbst die kontobezogenen Regelungen sich auf den Zahlungsverkehr beschränken. Art. 54 PSD2 über die Vertragsänderung bezieht sich ausdrücklich nur auf die Informations- und allgemeinen Vertragspflichten in Art. 52 PSD2. Andere Kontovertragsänderungen sind davon (theoretisch) nicht erfasst. Auch bei der Kündigung geht es um den Rahmenvertrag über die Zahlungsdienste – auch wenn sie regelmässig Teil des Kontovertrages bilden. Weiter ist zu bedenken, dass die Teilnahme am Scheme voraussetzt, dass alle die gleichen Wettbewerbsbedingungen vorfinden (Rule 5.1), und dass dies nur der Fall ist, wenn die Zahlungsdienstleister, die sich an SEPA beteiligen, auch im Hinblick auf die Kontoführung denselben Bedingungen unterliegen. Zudem enthält Rule 5.14 die Verpflichtung, soweit möglich von der Ausübung von Rechten abzusehen, die der PSD widersprechen. Der Wortlaut von Rule 5.14 Abs. 2 enthält – anders als Rule 5.14 Abs. 1 – keine Einschränkung im Hinblick auf das SEPA-Überweisungssystem. Es besteht also die Erwartung eines *best effort* zur Einhaltung aller Bestimmungen in Titel III und IV der PSD2. Soweit es also die Schweizer Banken selbst in der Hand haben und nicht aufgrund der regulatorischen Strukturen daran gehindert sind, PSD-konform zu agieren, kann man darin eine Verpflichtung sehen, auch die kontobezogenen Bestimmungen in Titel III und IV der PSD2 einzuhalten.

98 CTSR 2017 Rule 5.14.

Insgesamt ist wohl davon auszugehen, dass die SEPA-Verpflichtung der Schweizer Banken auch die (wenigen) kontorelevanten Bestimmungen der PSD2 mit umfasst. Damit bleibt es bei den Unterschieden zwischen den AGB der Schweizer Banken und den Vorgaben der PSD2 bei den kontorelevanten Bestimmungen.

V. Ausgewählte Eckpunkte in Titel IV der PSD2

Titel IV der PSD2 enthält den Kern des PSD-Privatrechts, nämlich die Regeln über die inhaltliche Ausgestaltung des Zahlungsdienstevertrages. Es ist im Wesentlichen ein privatrechtliches Verbraucherschutzrecht für die Rechtsbeziehung im Zahlungsverkehr.

Um die Stossrichtung der PSD2 zu verdeutlichen, sollen nachfolgend drei typische Störfälle und deren Lösung in der PSD2 vorgestellt werden. Dies erlaubt einen Vergleich mit den schweizerischen Lösungen. Da es insgesamt um Zahlungsvorgänge geht und auf der Dienstleisterseite die Banken stehen, wird der Einfachheit halber von Banken (statt Zahlungsdienstenbieter) und Kunden (statt Zahlungsdienstnutzer) gesprochen.

1. Nicht erfolgte, fehlerhafte oder verspätete Ausführung des Zahlungsvorgangs

Im ersten Störfall geht es darum, dass ein Zahlungsvorgang ordnungsgemäss in Auftrag gegeben wurde, anschliessend aber ein Fehler passiert: Die Zahlung wird nicht[99], fehlerhaft[100] oder verspätet ausgeführt.

a) Regelung in der PSD2

Die Grundregel der PSD2 lautet: Wenn auf der Ebene der Banken ein Fehler passiert ist, so ist dieser auf der Ebene der Banken zu beheben, und zwar unverzüglich.

---

99 Nicht erfolgt ist die Zahlung, wenn mit ihrer Ausführung nicht begonnen wurde oder wenn der Zahlungsbetrag innerhalb der Zahlungskette verloren gegangen ist. MüKo-BGB ZETSCHE, § 675y BGB N 9.

100 Fehlerhaft ist z.B. eine Zahlung, bei der eine unberechtigte Kürzung erfolgt ist, oder wenn sie an eine falsche Person erfolgt ist. MüKo-BGB ZETSCHE, § 675y BGB N 10.

Die PSD2 stellt klar, dass in diesen Fällen die kontoführende Bank haftet, ausser sie könne nachweisen, dass der Betrag bei der Empfängerbank ordnungsgemäss eingegangen ist.[101] Kann sie dies nicht, so hat die kontoführende Bank im Falle einer nicht oder fehlerhaft vorgenommenen Zahlung den Betrag unverzüglich zu erstatten bzw. wieder gutzuschreiben, mit Wertstellung zum Datum der Belastung.[102] Kann sie die ordnungsemässe Zahlung nachweisen, haftet die Empfängerbank, und sie muss dem Zahlungsempfänger den Betrag unverzüglich gutschreiben, mit Wertstellung auf den Zeitpunkt der ordnungsgemässen Gutschrift.[103]

Bei einer verspäteten Ausführung des Zahlungsauftrags[104] muss die Empfängerbank auf Verlangen der Zahlerbank sicherstellen, dass der Betrag auf dem Zahlungskonto des Zahlungsempfängers spätestens zu dem Datum wertgestellt wird, zu dem der Betrag bei korrekter Ausführung wertgestellt worden wäre. Mit anderen Worten: Den Banken wird die Verantwortung übertragen, dass Fehler bei der Erfüllung der Dienstleistung auf der Dienstleisterstufe behoben werden.

Die Banken haften darüber hinaus für alle von ihnen zu verantwortenden Entgelte und für Zinsen, die dem Kunden infolge einer nicht erfolgten, einer fehlerhaften oder eine verspäteten Ausführung in Rechnung gestellt werden.[105] Zu den Entgelten gehören die in Rechnung gestellten Entgelte für die Transaktion oder die Entgelte, die aufgrund der fehlerhaften Zahlung sonst entstehen können, z.B. Kontoüberziehungsgebühren.[106]

Die nationalen Rechtsordnungen können weitergehende Entschädigungsansprüche vorsehen.[107] Unabhängig von dieser Haftung ist die Bank verpflichtet, sich auf Verlangen des Kunden zu bemühen, den Zahlungsvorgang zurückzuverfolgen und den Zahler über das Ergebnis zu unterrichten. Er darf dem Zahler dafür kein Entgelt in Rechnung stellen.[108]

---

101 Art. 89 Abs. 1 PSD2.

102 Art. 89 Abs. 1 Unterabsatz 1.

103 Art. 89 Abs. 1 Unterabsatz 4 und 5.

104 Nach der PSD2 (und schon der PSD1) ist die Ausführungsfrist T+1, der Zahlungsbetrag muss also spätestens am Ende des auf den Zugangszeitpunkt des Zahlungsauftrags folgenden Geschäftstags bei der Empfängerbank eingehen, Art. 83 Abs. 1 PSD2.

105 Art. 89 Abs. 3 PSD2. Siehe dazu LINARDATOS, WM 2014, S. 305.

106 PALANDT BGB-SPRAU, § 675y N 17.

107 Art. 91 PSD2.

108 Art. 89 Abs. 1 Unterabsatz 7.

b) Regelung in den AGB der Schweizer Banken

In der Schweiz lautet die Standardklausel für die fehlerhafte Ausführung der Zahlungsaufträge wie folgt: «Werden Aufträge (ausgenommen Börsenaufträge) mangelhaft oder zu Unrecht nicht bzw. nicht rechtzeitig ausgeführt und entsteht ein Schaden, haftet [die Bank] für den Zinsausfall, es sei denn, dass sie im Einzelfall auf die drohende Gefahr eines darüber hinausgehenden Schadens aufmerksam gemacht worden ist.»

Die Handlungspflicht der Bank reduziert sich also im Regelfall auf die Erstattung des Zinsschadens. Es gibt keine Handlungspflicht zur unverzüglichen Gutschrift und vor allem gibt es keine interne Kompensations- und Abstimmungspflicht zwischen den Banken bei einer verspäteten Zahlung. Schliesslich fehlt auch die Pflicht zur unverzüglichen kostenlosen Nachforschung.

c) Fazit

Vergleicht man die Pflichtenlage bei nicht erfolgten, fehlerhaften oder verspäteten Zahlungsausführungen, so lässt sich nicht übersehen, dass der Pflichtenkatalog gemäss PSD2 für die Banken deutlich umfangreicher ausfällt. Die Pflichten könnten auch im schweizerischen Recht ohne Weiteres aus der auftragsrechtlichen Treuepflicht abgeleitet werden. Aber im Blueprint für die Bank/Kundenbeziehung, nämlich in den AGB, sind diese Pflichten nicht ausdrücklich festgehalten. Im Ergebnis bestehen also für den hier behandelten Störfall noch einige Unterschiede zwischen der Regelung in der PSD2 und dem schweizerischen Lösungsansatz.

2. Fehlerhafte Kundenidentifikatoren

Der zweite Störfall betrifft die fehlerhaften Kundenidentifikatoren, sprich: die Eingabe einer falschen IBAN. Der Hintergrund dieser Regel ist, dass die Abgleichung der IBAN des Empfängers mit dessen Namen nicht mehr vorgeschrieben ist, weil sonst die kurzen Ausführungsfristen (Gutschrift bis Ende des folgenden Geschäftstages)[109] nicht eingehalten werden könnten.[110]

[109] Art. 83 Abs. 1 PSD2.

Ein solcher Fehler wird allerdings ausserordentlich selten auftreten, weil die IBAN eine Prüfziffer enthält und einfache Verschreiber vom Banksystem sofort erkannt werden.[111]

Kommt es allerdings trotzdem zur Zahlung, weil der Verschreiber zufällig einer tatsächlich existierenden IBAN entspricht, so stellt sich die Frage nach den Rechten und Pflichten der involvierten Parteien.

a) Regelung in der PSD2

Wie oben erwähnt, gilt nach der PSD2, dass die Bank die Überweisung allein anhand der Kundenkennung vornehmen kann und eine solche Überweisung als ordnungsgemäss ausgeführt gilt[112] – mit der Konsequenz, dass der Bank ein Aufwendungsersatz gegenüber der anweisenden Kundin zusteht. Hat die Kundin eine falsche IBAN angegeben und ist die Zahlung erfolgt,[113] hat sie den Fehler zu vertreten. Sie hat weder einen Anspruch gegen ihre Bank,[114] noch gegen die Bank des (fehlerhaft genannten) Empfängers. Ihr bleiben nur bereicherungsrechtliche Ansprüche gegen den (falschen) Empfänger,[115] von dem sie aber lediglich die IBAN kennt. Einer Auskunft zur Identität des Empfängers steht aber das Bankgeheimnis der Empfängerbank entgegen, das diese auch gegenüber der kontoführende Bank geltend machen kann, falls letztere die Anfrage für die Kundin vornimmt.[116] Vor diesen Hintergrund trifft die PSD2 folgende Lösung:

Die kontoführende Bank wird verpflichtet, sich im Rahmen des Zumutbaren um die Wiedererlangung des Geldbetrages zu bemühen.[117] Sodann

---

110 So die Begründung der Bundesregierung zum Umsetzungsgesetz für die PSD1, BT-Drucksache 16/11643 vom 21.01.2009, S. 110 (Die Ausführung nach der Kundenkennung sei erforderlich, um die verkürzten EWR-weiten Ausführungsfristen zu ermöglichen). Zu dieser Begründung auch HOFFMANN, WM 2016, S. 1110.

111 Hoffmann, WM 2016, S. 1111. Zu den Prüfzifferberechnungsverfahren siehe die Nachweise bei BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, Rn. C/44.

112 Art. 88 Abs. 1 PSD2.

113 Zu den anderen Konstellationen siehe HOFFMANN, WM 2016, S. 1111 ff.

114 Art. 88 Abs. 1 und 2 PSD2.

115 So Auch PSD2 Erw. 88.

116 Für die Einzelkonstellationen im Rahmen der deutschen Regelung siehe BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, Rn. C/43 ff.

117 Art. 88 Abs. 3 PSD2. Siehe auch § 675y Abs. 5 Satz 2 BGB. Hierfür kann die Bank ein Entgelt verlangen, siehe Art. 88 Abs. 4 PSD2 und § 675y Abs. 5 Satz 5 BGB.

sieht die Richtlinie vor, dass die Bank des Zahlungsempfängers sich an den Bemühungen zur Wiedererlangung beteiligt, und zwar unter anderem dadurch, dass er der kontoführenden Bank alle für die Wiedererlangung massgeblichen Informationen mitteilt.[118] Mit anderen Worten wird für die Fälle einer Zahlung mit falscher Kundenkennung das Bankgeheimnis zurückgedrängt und die Empfängerbank wird zur «Zusammenarbeit» mit der Zahlerbank verpflichtet.[119] Diese Zusammenarbeit besteht «auch» in der Weitergabe der Empfängerinformationen. Daraus wird geschlossen, dass die Mitwirkungspflichten der Empfängerbank sich auf weitere Mitwirkungshandlungen erstreckt, wobei deren Umfang noch nicht abschliessend geklärt ist.[120]

Die Informationen bleiben in diesem Rahmen bei der Bank des Kunden und werden nicht an diesen weitergegeben. Nur für den den Fall, dass die Wiedererlangung des Geldbetrages scheitert, hat der Kunde einen Anspruch darauf, dass ihm seine Bank alle ihr verfügbaren Informationen mitteilt, damit der Kunde selbst seine Ansprüche gegen den (falschen) Empfänger geltend machen kann.[121] Aus den Mitwirkungspflichten der Empfängerbank schliessen einige Autoren sodann auf eine rechtliche (Sonder-)verbindung zwischen der anweisenden Kundin und der Empfängerbank.[122]

b) Regelung in den AGB der Schweizer Banken

Ein Blick auf die AGB von mehreren Schweizer Banken zeigt, dass zwar die SEPA-Überweisung geregelt ist. Sie beschränkt sich allerdings regelmässig auf die notwendigen Angaben für eine SEPA-Überweisung. Die Frage der falschen IBAN-Kennung wird nur zum Teil geregelt. Wo sich eine Regel

---

118 Art. 88 Abs. 3 PSD2. Noch weitergehend § 675y Abs. 5 Satz 3 BGB, der von einer «Verpflichtung» des Zahlungsdienstleisters des Zahlungsempfängers spricht.

119 PSD2, Erw. 88.

120 Die Umsetzung in § 675y Abs. 5 Satz 3 BGB sieht nur die Mitwirkungspflicht i.S.d. Informationslieferung vor. Für weiterführende Mitwirkungspflichten aber BÖGER, Neue Rechtsregeln, S. 292 und HOFFMANN, WM 2016, S. 1115 f. Die Pflichten sollen etwa die Aufforderung an den Zahlungsempfänger beeinhalten, der Rückleitung des Betrags zuzustimmen. Einem Stornorecht der Empfängerbank stehen beide Autoren kritisch gegenüber.

121 Art. 88 Abs. 3 Unterabsatz 2 PSD2.

122 HOFFMANN, WM 2016, S. 1114; zustimmend BÖGER, Neue Rechtsregeln, S. 292.

findet, lautet sie wie folgt: «Bei Verwendung der IBAN ist der Kunde sowohl als Auftraggeber als auch als Zahlungsempfänger damit einverstanden, dass die Verarbeitung des Zahlungsauftrages einzig anhand der IBAN erfolgt.» Unterstützungspflichten seitens der Zahlerbank oder der Empfängerbank sind nicht vorgesehen.[123]

c) Fazit

Die Grundregeln im Störfall «falsche Kundenidentifikatioren» sind unter der PSD2 und den AGB von Schweizer Banken dieselben. Eine Zahlung unter Verwendung einer gültigen IBAN darf ausgelöst werden. Die AGB der Schweizer Banken machen hier halt, während die PSD2 explizit eine Pflicht der Banken statuiert, den Kunden bei der Wiedererlangung seiner Gelder zu unterstützen.

3. Legitimationsmängel (nicht autorisierte Zahlungsvorgänge)

Der letzte Störfall betrifft die Legitimationsmängel. Das ist gleichzeitig der zentrale Störfall, weil mit der Verbreitung des Online-Banking die Betrugsfälle zunehmen. Nach der PSD gilt ein Zahlungsvorgang nur dann als autorisiert, wenn der Zahler der Ausführung des Zahlungsvorgangs zugestimmt hat. Fehlt die (vorgängige oder nachträgliche) Zustimmung, so gilt der Zahlungsvorgang als nicht autorisiert.[124] Nicht autorisiert sind namentlich Zahlungen, die einen Legitimationsmangel aufweisen, die also aufgrund einer unbefugten Nutzung der Legitimationsinstrumente des Zahlers erfolgen (z.B. Hacking, Diebstahl oder sonstige unbefugte Nutzung der Kontozugangsmittel).[125]

---

123 Anders bei Anwendbarkeit des SWIFT-Verfahrens, siehe dazu BGE 126 III 20.

124 Art. 64 Abs. 1 und 2 PSD2. Das bedeutet auch, dass im Privatrecht der Mitgliedstaaten (namentlich in Deutschland) Rechtsscheinsgrundsätze wie die Duldungs- und Anscheinsvollmacht wegen des Vorrangs des europäischen Rechts zurücktreten müssen. Siehe BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, Rn. C/35 m.w.N. (insb. auch BGH XI ZR 91/14 vom 26. Januar 2016 = BGH, NJW 2016, 2024 Rn. 58 ff.).

125 Die PSD2 spricht in diesem Zusammenhang von «Zahlungsinstrumenten», siehe Art. 74 Abs. 1 PSD2.

a) Regelung in der PSD2

Die PSD2 folgt bei der rechtlichen Erfassung eines Legitimationsmangels folgender Grundstruktur: Wenn die Bank an einen Unbefugten leistet, hat sie nicht richtig erfüllt. Der Kunde hat einen Erstattungsanspruch gegen die Bank, denn diese schuldet ihm nach wie vor ihre Leistung. Konkret: Sie muss den abgebuchten Betrag wieder gutschreiben. Die Bank erleidet dadurch im Normalfall einen Schaden, denn sie hat den Betrag bereits überwiesen und müsste ihn vom Empfänger zurückholen, was schwierig ist, wenn es sich um einen Betrüger handelt. Sie hat aber gegebenenfalls für diesen Schaden einen Ersatzanspruch gegen den Kunden. Dies ist dann der Fall, wenn der Kunde pflichtwidrig zum Schaden der Bank beigetragen hat, zum Beispiel, indem er seine Zugangsdaten nicht sorgfältig aufbewahrt hat.

Die PSD2 konkretisiert das Zusammenspiel von Erstattungspflicht der Bank und Schadenersatzpflicht des Kunden in mehreren Bestimmungen. Die grundsätzliche Stossrichtung des Regelungsansatzes wird folgendermassen zusammengefasst: «Das Risiko für eine nicht autorisierte ('missbräuchliche') Zahlung trägt der Zahlungsdienstleister des Zahlers.»[126]

aa) Erstattungspflicht der Bank

Erstens muss die Bank, sobald die Kundin eine nicht autorisierte Belastung geltend macht, den Betrag unverzüglich, nämlich bis zu nächsten Geschäftstag, wieder gutschreiben. Eine Ausnahme gilt nur, wenn die Bank sie berechtigte Gründe für den Verdacht hat, dass seitens des Kunden ein Betrug vorliegt. Selbst in diesem Fall darf sie die Gutschrift nur verweigern, wenn sie der Behörde eine entsprechende Meldung erstattet.[127] Die Schwelle wird also sehr hoch gelegt. Im Ergebnis muss die Bank den Betrag zunächst wieder gutschreiben.

---

126 BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, Rn. C/54. Zur Rechtslage im deutschen Recht vor der PSD1 (Bereicherungsansprüche) siehe DIECKMANN, WM 2015, S. 14 ff.; Piekenbrock, WM 2015, S. 797 ff.

127 Art. 73 Abs. 1 PSD2. Der Absatz stellt zudem auch klar, dass das Konto auf den Zeitpunkt der (unautorisierten) Belastung wertgestellt werden muss. Sodann können gemäss Art. 73 Abs. 3 PSD2 die nationalen Rechtsordnungen weitergehende Ansprüche des Zahlers gegen den Zahlungsdienstleister vorsehen.

Was den weiteren Verlauf der Auseinandersetzung angeht, so muss die Bank gegenüber dem Kunden namentlich nachweisen, dass der Zahlungsvorgang authentifiziert, ordnungsgemäss aufgezeichnet und nicht durch ei-eine technische Panne oder einen anderen Mangel beeinträchtigt wurde.[128] Die Authentifizierung gilt als erfolgt, wenn die Bank die Nutzung der vereinbarten Authentifizierungsinstrumente, namentlich also die Verwendung der persönlichen Sicherheitsmerkmale,[129] ordnungsgemäss überprüft hat. Sind diese Voraussetzungen nicht erfüllt, gilt die Zahlung als nicht autorisiert.

Selbst wenn die richtigen Legitimationsmittel, also die richtige PIN und TAN verwendet wurde, heisst das nicht automatisch, dass die Zahlung autorisiert war. Das ordnungs- und systemgemässe Transaktionsprotokoll erfüllt lediglich die Mindestvoraussetzungen dafür, dass die Zahlung nicht von vornherein als nicht autorisiert qualifiziert wird. Die PSD2 hält ausdrücklich fest, der Nachweis einer ordnungsgemässen Authentifizierung reiche «für sich gesehen nicht notwendigerweise aus», um eine Autorisierung durch den Kunden zu belegen.[130] Die beweisrechtliche Konkretisierung erfolgt durch die Gerichte der Mitgliedstaaten.

Orientiert man sich an der deutschen Rechtsprechung, so ist die Hürde sehr hoch. Die Formel «für sich gesehen nicht notwendigerweise» wurde von einigen Gerichten so ausgelegt, dass die Verwendung der korrekten Zugangsdaten generell keinen prima-facie Beweis (Anscheinsbeweis) für die Autorisierung durch den Kontoinhaber liefert, während andere Gerichte bei gewissen Authentifizierungsverfahren (smsTAN, chipTAN) einen solchen Beweis zuliessen.[131] Der BGH hat sich in einer Entscheidung aus dem Jahr

---

128 Art. 72 Abs. 1 Unterabsatz 2 PSD2.

129 Für andere Beispiele siehe PALANDT BGB-SPRAU, § 675w N 3: Eingang des Zahlungsauftrags auf dem vereinbarten Weg, Überprüfung von Sicherheitsmerkmalen, Kundenennummer und PIN bei Abhebung am Geldautomaten, Überprüfung von Kundenkennung, PIN und TAN beim Onlinebanking, Abfage von Kundenkennung und Kennwort im Telephonbanking.

130 Art. 72 Abs. 2 PSD2.

131 Übersicht zur Rechtsprechung bei HOEREN/KAIRIES, WM 2015, S. 549 ff. Für eine Kurzfassung HOEREN/KAIRIES, ZBB 2015, S. 35 Fn. 1 (kein Anscheinsbeweis) und S. 37 Fn. 13 und 15 (Anscheinsbeweis für das smsTAN und das chipTAN-Verfahren bejaht, wobei jeweils subsidiär eine grobe Fahrlässigkeit angenommen wurde). Anschaulich – auch im Hinblick auf den Ablauf einer Hacking-Attacke – ist in diesem Zusammen-

2016 aber dahingehend geäussert, dass ein Anscheinsbeweis im Falle der korrekten Authentifizierung nicht gänzlich ausgeschlossen ist. Voraussetzung ist allerdings, dass auf der Grundlage aktueller Erkenntnisse die allgemeine praktische Unüberwindbarkeit des eingesetzten Sicherungsverfahrens sowie dessen ordnungsgemässe Anwendung und fehlerfreie Funktion im konkreten Fall feststehen. Der Kunde muss zur Erschütterung dieses Anscheinsbeweises sodann keinen konkreten und erfolgreichen Angriff gegen das Authentifizierungsinstrument (PIN, TAN) vortragen und beweisen, sondern er kann sich auch auf andere Umstände stützen, die für einen nicht autorisierten Zahlungsvorgang sprechen (z.B. geographische Entfernung vom Computer, von dem aus die Zahlung ausgelöst wurde).[132]

Im Ergebnis kommt es also, wenn der Kunde eine nicht autorisierte Zahlung geltend macht, in einem ersten Schritt zu einer unverzüglichen Erstattungspflicht der Bank. Im zweiten Schritt stellt sich dann die Frage nach dem Schadenersatzanspruch der Bank gegenüber dem Kunden.

bb) Schadenersatzanspruch gegenüber dem Kunden

Die Bank hat für den Schaden, der ihr aufgrund der unverzüglichen Erstattungspflicht entsteht, grundsätzlich einen Schadenersatzanspruch gegenüber dem Kunden. Diese ist stufenweise geregelt.

---

hang ein Entscheid des LG Köln, Urt. v. 26.8.2014 – 3 O 390/13, WM 2014, S. 2372, NJW 2014, S. 3735: Der Kunde erhielt eine Meldung, das Online-Konto sei momentan nicht verfügbar. Er liess das Konto sperren, überprüfte seine Firewall-Einstellungen und seine Antiviren-Software. Das Konto wurde wieder freigeschaltet, es enthielt keine Unregelmässigkeiten. Einige Tage später wollte der Kunde eine Überweisung tätigen. Da erschien auf der Banking-Portal-Seite die Meldung, dass die Sicherheitseinstellungen auf Grund der vorübergehenden Sperrung neu überprüft werden müssen. Dem Kunden wurde «Sicherheitstest jetzt ausführen» angezeigt, die dieser mit «Ja» bestätigte. Danach erschien auf dem Handy des Kunden eine TAN für eine Überweisung im Betrag, den der Kunde vorher hatte überweisen wollen. Die IBAN erwies sich aber im Nachhinein als falsch. Der Kunde führte diese Zahlung aus und danach noch die anfangs geplante Überweisung. Das Gericht hielt dafür, dass die erste Zahlung entweder autorisiert war, oder dass sie grob fahrlässig verursacht wurde, weil der Kunde die IBAN nicht abeglichen hatte. Zum chipTAN-Verfahren siehe LG Darmstadt, Urt. v. 28.08.2014 - 28 O 36/14, WM 2014, S. 2323 (Beschreibung des chipTAN-Verfahrens).

132 BGH XI ZR 91/14 vom 26. Januar 2016 = NJW 2016, S. 2024 Rn. 20 ff., insb. Rn. 38. Im Entscheid ging es um ein smsTAN-Verfahren. Der BGH weist diesbezüglich auf bekanntgewordene Sicherheitslücken hin.

Den Kunden trifft eine volle Schadenersatzpflicht, wenn er in betrügerischer Absicht gehandelt hat.[133] In diesem Zusammenhang gilt wiederum die Beweislastregel, wonach die ordnungsgemässe Authentifizierung und die ordnungsgemässe Aufzeichnung des Zahlungsvorgangs nicht genügt, um dem Kunden eine betrügerische Absicht zu unterstellen. Die PSD2 hält weitergehend fest, dass die Bank «unterstützende Beweismittel» vorlegen muss, wenn sie den Betrug des Kunden nachweisen will.[134]

Den Kunden trifft weiter eine volle Schadenersatzpflicht, wenn er grob fahrlässig seine Sicherungs- und Anzeigepflichten verletzt hat.[135] Allerdings verliert die Bank selbst in diesem Fall ihren Schadenersatzanspruch, wenn sie keine starke Kundenauthentifizierung verlangt hat.[136] Man schafft mithin über die Risikoverteilung einen weiteren Anreiz zur Implementierung der geforderten Sicherheitsstandards.

Bei leichtem Verschulden haftet der Kunde für einen Höchstbetrag von 50 Euro.[137] Wenn ihn gar kein Verschulden trifft, so entfällt die Haftung auch im Umfang des Höchstbetrages. [138]

cc) Fazit

Die PSD2 geht vom Grundsatz der Erstattungspflicht der Bank aus und richtet dann den Blick auf das Kundenverhalten, um festzustellen, ob die Bank verrechnungsweise einen Schadenersatz geltend machen kann. Sie verknüpft die Erstattungspflicht aber mit den technischen Sicherheitsanforderungen und bestraft über das Haftungsregime diejenigen Banken, welche die vorgesehenen Sicherheitsstandards nicht umsetzen.

---

133 Art. 74 Abs. 1.

134 Art. 72 Abs. 2 PSD2.

135 Art. 74 Abs. 1 Unterabsatz 3.

136 Art. 74 Abs. 2 PSD2.

137 Der Maximalbetrag verdeutlicht, dass es nicht um eine effektive Kostenerstattung geht, sondern um eine Präventionsmassnahme, die Anreize für eine Risikobegrenzung seitens des Kunden setzen soll. So auch BÖGER, Neue Rechtsregeln, S. 294. Gemäss LINARDATOS, WM 2014, S. 303, wird sich aufgrund der geringen Summe seitens der Banken ein rationales Desinteresse an der Geltendmachung dieses Anspruchs einstellen.

138 Art. 74 Abs. 1 lit. a PSD2: «wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments für den Zahler vor einer Zahlung *nicht bemerkbar* war, es sei denn, der Zahler hat selbst in betrügerischer Absicht gehandelt.».

b) Regelung in den AGB der Schweizer Banken

In der Schweiz ist die Rechtslage im Ausgangspunkt mit der Regelung in der PSD2 vergleichbar. Wenn die Bank an einen Unbefugten leistet, so hat sie nicht mit Befreiungswirkung geleistet. Sie schuldet daher den unbefugt abgezogenen Betrag weiterhin.[139] Sie hat aber ihrerseits einen verschuldensabhängigen Schadenersatzanspruch gegen den Kunden.[140] Diese Regelung wird aber in den Banken-AGB durchweg modifiziert. Das gilt insbesondere auch beim heute praktisch wichtigsten Fall der Legitimationsmängel, also beim Online-Banking.

aa) Legitimationsabreden

Betrachtet man die Banken-AGB im Online-Banking, so scheitert ein Erstattungsanspruch des Kunden in der frühstmöglichen Phase. Die AGB der Banken sehen durchweg vor, dass dass Aufträge und Mitteilungen von Personen, die sich mit dem vorgesehenen Legitimationsverfahren Zugang zu den Online-Dienstleistungen der Bank verschafft, als vom Kunden verfasst bzw. als von ihm autorisiert gelten. Die Bank ist ermächtigt, diesen Instruktionen Folge zu leisten.[141] Teilweise wird präzisiert, dass der Kunde vorbehaltlos alle auf seinen Konten verbuchten Transaktionen anerkennt, die mittels E-Banking-Dienstleistungen in Verbindung mit seinen/ihren Le-

---

139 BGE 112 II 450 E. 4 S. 457; 132 III 450 E. 2 S. 452; BGer Urteil 4C.377/2000 vom 8. März 2001 E. 1b; 4C.28/2003 vom 15. Dezember 2003 E. 3.2.1; 4A_386/2016 vom 5. Dezember 2016 E. 2.2.2. Aus jüngerer Zeit zudem SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

140 BGer 4A_438/2007 vom 29. Januar 2008 E. 5.1; SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

141 AGB-Beispiel: «Jede Person, die sich mit den persönlichen Legitimationsmitteln und dem in der «Anleitung» beschriebenen Legitimationsverfahren erfolgreich Zugang zu [Bank] Digital Banking verschafft (Selbstlegitimation), gilt der [Bank] gegenüber als zugriffsberechtigt; dies gilt unabhängig davon, ob es sich bei dieser Person tatsächlich um den Zugriffsberechtigten handelt bzw. diese vom Vertragspartner entsprechend autorisiert wurde. Sämtliche bei [Bank] über [Bank] Digital Banking eingehenden Weisungen und Instruktionen gelten als vom Zugriffsberechtigten verfasst. [Bank] gilt als beauftragt, im Rahmen des üblichen Geschäftsgangs diese Weisungen auszuführen sowie den Mitteilungen nachzukommen, sobald diesen eine korrekte Legitimationsprüfung zugrunde liegt.» (Stand: 1. Juni 2018).

gitimationsverfahren getätigt worden sind.[142] Weitergehende Konkretisierungen zur Legitimationsabrede führen aus, diese bedeute, dass der Zugriffsberechtigte die Risiken trägt, die sich (i) aus Manipuliationen an dessen EDV-System durch Unbefugte, (ii) aus missbräuchlicher Verwendung der persönlichen Legitimationsmittel, (iii) aus Verletzung von Sorgfaltspflichten oder (iv) aus Eingriffen unberechtigter Dritter in die Datenübermittlung ergeben. Hier wird also dem Kunden im Rahmen der Legitimationsabrede nicht nur die Sphärenhaftung, sondern auch die Zufallshaftung (Eingriff in Datenübermittlung) übertragen.

Im Online-Banking ist damit für alle erdenklichen Fälle von missbräuchlicher Verwendung der Zugangsdaten eine Erstattungspflicht der Bank ausgeschlossen. Damit endet an sich die Frage nach der Haftungsverteilung bei Legitimationsmängeln im E-Banking, dem heute mit Abstand häufigsten Fall von Legitimationsmängeln.

Nun verstossten allerdings diese absolut formulierten Klauseln gegen Art. 8 UWG. Denn sie lassen den Kunden auch in denjenigen Fällen das Risiko tragen, in denen der Missbrauch der Zugangsdaten in den Verantwortungsbereich der Bank fällt, etwa weil sie eine Sicherheitslücke in ihrer verschlüsselten Kommunikation mit dem Kunden zu verantworten hat, oder weil in ihrem System die Zugangsdaten abgefragt und manipuliert wurden, oder weil es eine erfolgreiche Man-in-the-Middle-Attacke gab und sich der Angreifer vor die Bank geschoben und so die Zahlungen manipuliert hat. In einer solch einseitigen Risikoverteilung liegt ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und Pflichten, das in treuwidriger Weise zum Nachteil des Kunden ausgestaltet ist. Nur muss der Kunde den Verstoss gegen Art. 8 UWG zunächst einmal vor einem Gericht geltend machen.

Falls er erfolgreich ist und die entsprechend Klausel als nichtig erklärt wird, ist aber keineswegs sicher, dass die Bank ihm den unbefugt abgezogenen Betrag wieder erstatten muss. Denn in diesem Fall kommen im Regelfall

[142] AGB-Beispiel: «Der Kunde/Die Kundin anerkennt vorbehaltlos alls auf seinen/ihren Konten/Depots verbuchten Transaktionen, welche mittels E-Banking-Dienstleistungen in Verbindung mit seinen/ihren Legitimationsverfahren getätigt worden sind. Instruktionen, Aufträge und Mitteilungen, welche die [Bank] auf diesem Weg erreichen, gelten als vom Kunden/von der Kundin autorisiert.».

die allgemeinen Schadenersatzansprüche des Obligationenrechts zum Tragen. Oder es gelten ausnahmsweise die in den AGB vorgesehen Schadenabwälzungsklauseln.

bb) Schadenersatzansprüche der Bank

Fehlt es wegen Nichtigkeit an der Legitimationsabrede, wonach eine Zahlungsanweisung mittels vorgesehener Legitimationsmittel als autorisiert gilt, so kommen die allgemeinen Grundsätze des Obligationenrechts zum Tragen. Danach trifft die Bank eine Erstattungspflicht, sie hat aber ihrerseits bei gegebenen Voraussetzungen einen Schadenersatzanspruch gegen den Kunden.

Nach den allgemeinen Regeln des Obligationenrechts steht ihr ein solcher Schadenersatz bei *jedem* Verschulden des Kunden an der unautorisierten Zahlung zu (Art. 99 Abs. 1 OR) – etwa ein unsorgfältiger Umgang mit seinen Legitimationsmitteln oder eine versäumte Aktualisierung seiner Sicherheits-Updates. Anders als bei der PSD2 gelten also keine Abstufungen. Ein allfälliges eigenes Verschulden der Bank wird dann im Rahmen der Schadensberechnung (Art. 44 OR i.V.m. Art. 99 Abs. 3 OR) relevant. Das führt allenfalls zu einer Herabsetzung oder – im Ausnahmefall – zu einem gänzlichen Verlust des Schadenersatzanspruchs.

cc) Schadensabwälzungsklauseln

Je nach Ausgestaltung der AGB gelten neben den besonderen Bestimmungen zum Online-Banking die allgemeinen Basisbestimmungen der Bank als Auffangordnung. Dieser Fall wird selten eintreten, denn die Ausgestaltung der Online-Banking-Bestimmungen lassen erkennen, dass diese für Legitimationsmängel eine abschliessende Ordnung aufstellen. Häufig wird sodann bei der Regelung der Legitimationsmängel in den allgemeinen AGB der Banken auf den Fall der Prüfung der Unterschriften verwiesen, was zusätzlich untermauert, dass diese nicht auf das Online-Banking Anwendung finden sollen.

Mit der Schadensabwälzungsklausel, die sich standardmässig in den Banken-AGB findet, überwälzt die Bank den Schaden, der ihr aus einem Legitimationsmangel erwächst, auf den Kunden. Den Schaden erleidet die Bank deshalb, weil sie die unbefugte Zahlung dem Kunden nicht belasten kann und er vom (betrügerisch handelnden) Empfänger nicht erbringbar ist. Moderne Schadensabwälzungsklauseln lauten üblicherweise wie folgt:

«Leistet [die Bank] trotz Anwendung der üblichen Sorgfalt an Nichtberechtigte, haftet der Kunde/die Kunden für den entstandenen Schaden. Die Haftung des Kunden/der Kundin entfällt, wenn der Schaden auf Umstände zurückzuführen ist, die nicht in seinem/ihren Einflussbereich liegen.»[143]

Die Funktionsweise der Schadenabwälzungsklausel ist nicht abschliessend geklärt. Man kann sie dogmatisch verschieden einordnen:

– Sie beeinhaltet eine Einschränkung des Erfüllungsanspruchs des Kunden gegenüber der Bank. Diesfalls wird der Erfüllungsanspruch an bestimmte einschränkende Bedingungen geknüpft. Gemäss der oben erwähnten Klausel besteht er nur, wenn man der Bank eine Sorgfaltspflichtverletzung vorwerfen kann oder – bei fehlendem Verschulden der Bank – wenn die unautorisierte Zahlung ihren Ursprung im Einflussbereich (Risikobereich) der Bank hat.

– Sie berührt den Erfüllungsanspruch des Kunden gegen die Bank nicht, hingegen beeinhaltet sie einen Erfüllungsanspruch der Bank gegenüber dem Kunden auf Erstattung des Schadens, den die Bank erleidet, weil sie einem Unbefugten geleistet hat und sie denselben Betrag dem Kunden erstatten muss. Konkretisiert durch die obenerwähnte Klausel: Die Bank hat einen Erfüllungsanspruch gegenüber dem Kunden, wenn sie an der unautorisierten Zahlung kein Verschulden trifft, oder – bei fehlendem Verschulden der Bank – wenn die unautorisierte Zahlung in ihrem Einflussbereich (Risikobereich) ihren Ursprung hat.

– Sie berührt den Erfüllungsanspruch des Kunden gegen die Bank nicht. Der Gegenanspruch ist aber kein Erfüllungsanspruch der Bank, sondern ein Schadenersatzanspruch, der allerdings vertraglich modifiziert wird. Konkretisiert anhand der obenerwähnten Klausel: Die Modifikation besteht einerseits darin, dass der Herabsetzungsgrund des Selbstverschuldens der Bank (Art. 44 i.V.m. Art. 99 Abs. 3 OR) als Ausschlussgrund für den Schadenersatzanspruch wirkt. Andererseits wird der Schadenersatzanspruch dahingehend modifiziert, dass er auch dann greift, wenn den Kunden kein Verschulden trifft, aber die unautorisierte Zahlung seinem Einflussbereich (Risikosphäre) zuzuordnen ist.

[143] Teilweise sehen (überkommene) AGB von Banken vor, dass die Bank den Schaden nur selbst trägt, wenn sie ein grobes Verschulden trifft.

– Sie ist eine Kombination von modifiziertem Schadenersatzanspruch und Erfüllungsanspruch. Konkretisiert anhand der obenerwähnten Klausel: Der modifizierte Schadenersatzanspruch besteht darin, dass die Bank im Falle eines Selbstverschuldens auf den Anspruch verzichtet (Modifikation von Art. 44 i.V.m Art. 93 Abs. 3 OR). Der Erfüllungsanspruch besteht in der vertraglichen Abrede, dass der Kunde der Bank unhängig von seinem eigenen Verschulden den Schaden ersetzt, sofern sich die unautorisierte Zahlung seinem Risikobereich zuordnen lässt.[144]

Trotz langjähriger Rechtsprechung zu den Legitimationsmängeln sind die Fragen um die dogmatische Einordnung der Schadensabwälzungsklauseln noch weitgehend ungeklärt.[145] Sie bedürfen einer Analyse, die den Rahmen des vorliegenden Beitrags sprengen würde, zumal – wie eingangs erwähnt – die Schadensabwälzungsklauseln bei Legitimationsmängeln im Online-Banking nur im Ausnahmefall als Auffangregeln Anwendung finden.

Relevant ist hier die immer gleichbleibende Schlussfolgerung, dass bei Anwendung der Schadensabwälzungsklauseln die Bank im Ergebnis für die unautorisierte Zahlung nur einstehen muss, wenn sie ein Verschulden trifft oder wenn der Fehler in ihrer Risikosphäre liegt. Es kommt also immer auch auf die Bank und ihr Umfeld an. Das ist bei der PSD2 grundlegend anders.

c) Fazit

Man kann es drehen und wenden wie man will: Bei den Legitimationsmängeln ist die Stossrichtung der PSD2 eine grundlegende andere als bei dem AGB-Recht der Schweizer Banken.

Zusammengefasst ergibt sich nämlich: Bei der PSD2 gilt der Grundsatz der vollen Erstattungspflicht der Bank. Das ist der Ausgangspunkt. Der Fokus liegt dann auf dem Verhalten des Kunden. Wenn der Kunde sich betrügerisch oder grob fahrlässig verhält, haftet er voll. Wenn er sich leicht fahrlässig verhält, haftet er im Umfang von 50 Euro. Wenn ihn kein Verschulden trifft, haftet er nicht. So steht es auch in den AGB der EU-Banken: «Im Falle einer nicht autorisierten Überweisung … hat die Bank gegen den

144 Diese Variante trägt der Tatsache Rechnung, dass nach herkömmlicher Auffassung der vertragliche Schadenersatz jedenfalls eine Vertragsverletzung voraussetzt.

145 So auch EMMENEGGER/THÉVENOZ, SZW 2017, S. 221.

Kunden keinen Anspruch auf Erstattung ihrer Aufwendungen. Sie ist verpflichtet, dem Kunden den Überweisungsbetrag zu erstatten…»[146] Hinzu kommt, dass die Ersatzansprüche der Bank gegen den leicht oder grobfahrlässig handelnden Kunden scheitern, wenn sie die anspruchsvollen Sicherheitsstandards für Online-Zahlungsanweisungen nicht umgesetzt hat. In diesem Fall haftet nur der Kunde, der in betrügerischer Absicht gehandelt hat.

Im AGB-Recht der Schweizer Banken ist der Grundsatz umgekehrt. Grundsätzlich trägt der Kunde den Schaden, denn Zahlungsanweisungen unter Verwendung der vorgesehen Legitimationsmittel gelten als autorisiert. Es bedarf dann zuerst eines Gerichtsentscheids, der diese Klausel wegen eines Verstosses gegen Art. 8 UWG als (voll-)nichtig erklärt. Selbst in diesem Fall bleibt der Bank ein Schadenersatzanspruch gegen den Kunden gestützt auf das allgemeine Schadensrecht, sofern den Kunden am Legitimationsmangel irgendein Verschulden trifft (Art. 99 Abs. 1 OR). Ein allfälliges Eigenverschulden der Bank spielt erst auf der Stufe der Schadenersatzbemessung eine Rolle (Art. 44 OR). An diesem Ergebnis ändert sich nur wenig, falls – ausnahmsweise – die Legitimationsfragen in den Online-AGB nicht abschliessend geregelt sind und die Schadensabwälzungsklauseln der allgemeinen AGB zum Tragen kommen.

Wenn man bedenkt, dass die Schweizer Banken sich für den Bereich der Euro-Überweisungen zur Einhaltung des PSD2-Privatrechts verpflichtet haben, so zeigt sich bei den Legitimationsmängeln ein eklatanter Unterschied im Regelungsansatz.

VI. Zusammenfassung und Ausblick

Die EU hat mit der PSD2 ein umfassendes Regelwerk zu den Zahlungsdienstleistungen geschaffen. Was auffällt, ist die Konsequenz, mit der sie in diesem Bereich das Ziel des Binnenmarktes verfolgt. Man spürt förmlich, dass die 500 Mio. EU-Bürger sich an den Computer setzen und EU-weite Waren und Dienstleistungen erwerben sollen. Die konsequente Verfolgung

[146] So beispielsweise der deutsche Bankenverband, Mustertext, Bedingungen für den Übeweisungsverkehr, Ziff. 2.3.1 (Stand: 13. Januar 2018). Umgesetzt z.B. bei Bank Santander, Bedingungen für den Überweisungsverkehr, Ziff. 2.3.1.

des Binnenmarkt-Ziels zeigt sich auch in der inhaltlichen Ausgestaltung der PSD2: Man forciert hohe Sicherheitsstandards und einen hohen Verbraucherschutz. Der Preis dafür ist ein schwer verdauliches Regelwerk, das im Kundenverhältnis auch wenig individuellen Gestaltungsspielraum lässt. Man überlässt wirklich nichts dem Zufall.

Für die Schweizer Banken gibt es Anpassungsbedarf. Einerseits für den Euro-Überweisungsverkehr. Denn dazu haben sie sich verpflichtet, und die Kundinnen und Kunden können dies auch einfordern. Tatsächlich zeigen sich in diesem Bereich aber eklatante Unterschiede im Regelungsansatz, gerade auch bei möglichen Störfällen im Überweisungsverkehr.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 1. Mai 2018.

BAUMBACH/HOPT HGB-BEARBEITER, Handelsgesetzbuch mit GmbH & Co., Handelsklauseln, Bank- und Kapitalmarktrecht, Transportrecht (ohne Seerecht), hrsg. von Klaus J. Hopt u.a., 38. Aufl., München 2018.

BÖGER OLE, Neue Rechtsregeln für den Zahlungsverkehr, in: Volker Gross u.a. (Hrsg.), Bankrechtstag 2016, Berlin 2017, S. 193–300.

DIECKMANN ANDREAS, Die SEPA-Überweisung: eine unterschätzte Gefahr für die Banken, WM 2015, S. 14–22.

EMMENEGGER SUSAN, Unautorisierte Transaktionen im Zusammenhang mit Dritten Zahlungsdienstleistern, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 87–116.

EMMENEGGER SUSAN/FRITSCHI MIRJAM, Schweizer Banken: EU-Recht für EU-Kunden, in: Alexander R. Markus u.a. (Hrsg.), Zivilprozess und Vollstreckung national und international – Schnittstellen und Vergleiche, Bern 2018, S. 75–92.

EMMENEGGER SUSAN/THÉVENOZ LUC, Le droit bancaire privé suisse 2017 – Das schweizerische Bankprivatrecht 2017, SZW 2018, S. 184–214.

EMMENEGGER SUSAN/THÉVENOZ LUC, Das schweizerische Bankprivatrecht 2016 – Le droit bancaire privé suisse 2016, SZW 2017, S. 210–247.

EMMENEGGER SUSAN/THÉVENOZ LUC, Das schweizerische Bankprivatrecht 2014–2015 – Le droit bancaire privé suisse 2014–2015, SZW 2015, S. 386–416.

FINDEISEN MICHAEL, Das Zahlungskontengesetz – Auftrieb für den modernen Zahlungsverkehr und den Verbraucherschutz, WM 2016, S. 1765–1774.

FOUNTOULAKIS CHRISTINA, Der Vertrag mit Schutzwirkung für Dritte, AJP 2018, S. 95–99.

GAUCH PETER/SCHLUEP WALTER R./SCHMID JÖRG/EMMENEGGER SUSAN, Schweizerisches Obligationenrecht, Allgemeiner Teil, Bd. II, 10. Aufl., Zürich 2014.

GRUNDMANN STEFAN, Das neue Recht des Zahlungsverkehrs – Teil I – Grundsatzüberlegungen und Überweisungsrecht, WM 2009, S. 1109–1117.

HESS MARTIN/KEISER BARBARA, Euro Zahlungen gemäss den SEPA-Rulebooks durch Schweizer Finanzinstitute, SZW 2009, S. 153–175.

HOFFMANN JOCHEN, Die Überweisung anhand fehlerhafter Kundenkennung unter der Neufassung der Zahlungsdiensterichtlinie, WM 2016, S. 1110–1118.

HOEREN THOMAS/KAIRIES MARIA, Anscheinsbeweis und chipTAN, ZBB 1/2015, S. 35–40.

HOEREN THOMAS/KAIRIES MARIA, Der Anscheinsbeweis im Bankenbereich – aktuelle Entwicklungen, WM 2015, S. 549–553.

JURI GABRIEL, Single Euro Payments Area – Registration process is launched, ClearIT December 2007, S. 7.

KRAUSKOPF PATRICK, Der Vertrag zugunsten Dritter, Diss. Freiburg 2000.

LINARDATOS DIMITRIOS, Der Kommissionsvorschlag für eine Zahlungsdiensterichtlinie II – Ein Überblick zu den haftungsrechtlichen Reformvorhaben, WM Heft 7/2014, S. 300–307.

LINARDATOS DIMITRIOS, Die Basiskonto-Richtlinie – ein Überblick, WM 2015, S. 755–762.

Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 5/2, Schuldrecht, Besonderer Teil III/2, §§ 651a–704 BGB, hrsg. von Martin Henssler, 7. Aufl., München 2017.

Oechsler Jürgen, Ein neuer wettbewerblicher Ordnungsrahmen für das Kreditkartengeschäft – MIF-VO, Zahlungsdiensterichtlinie 2 und die Mastercard-Entscheidung des EuGH, WM 2016, S. 537–542.

OMLOR SEBASTIAN, Die zweite Zahlungsdiensterichtlinie: Revolution oder Evolution im Bankvertragsrecht?, ZIP 12/2016, S. 558–564.

OMLOR SEBASTIAN, Entgelte im Zahlungsverkehr nach Umsetzung der Zweiten Zahlungsdiensterichtlinie (PSD II), WM 2018, S. 937–943.

OMLOR SEBASTIAN, Zahlungsdiensteaufsichtsrecht im zivilrechtlichen Pflichtengefüge, WM 2018, S. 57–63.

PALANDT BGB-BEARBEITER, Bürgerliches Gesetzbuch mit Nebengesetzen, hrsg. von Gerd Brudermüller u.a., 76. Aufl., München 2017.

PIEKENBROCK ANDREAS, Das Recht der Zahlungsdienste zwischen Unions- und nationalem Recht, WM 2015, S. 979–804.

SCHALLER JEAN MARC, Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Basel 2017, S. 45–70.

SCHMID FABIAN, (Starke) Kundenauthentifizierung: Aufsichtsrecht und Zivilrecht, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 67–85.

TERLAU MATTHIAS, Die zweite Zahlungsdiensterichtlinie – zwischen technischer Innovation und Ausdehnung des Aufsichtsrechts, ZBB 2/2016, S. 122–137.

Wandhöfer Ruth, EU Payments Integration. The Tale of SEPA, PSD and other Milestones along the Road, Palgrave Macmillan 2010.

WERNER STEFAN, Der Weg zu SEPA und die Auswirkungen auf die Zahlungsdienste – ein Überblick, WM 2014, S. 243–250.

Materialien

Bank Santander, Bedingungen für den Überweisungsverkehr, Stand: 1. Juni 2018

BEKB, Benutzung von E-Banking Dienstleistungen, in: Vertragliche Grundlagen für die Geschäftsbeziehungen mit der Berner Kantonalbank AG, 10 f.

BT-Drucksache 16/11643, Deutscher Bundestag, Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht, vom 21.01.2009.

Deutscher Bankenverband, Mustertext, Bedingungen für den Überweisungsverkehr, Stand: 13. Januar 2018.

Europäische Zentralbank (EZB), Einheitliche Euro-Zahlungsverkehrsraum (SEPA), Pressemitteilung vom 4. Mai 2006.

Europäische Zentralbank (EZB), SEPA-Fortschrittsbericht, Auf dem Weg zu einem einheitlichen Euro-Zahlungsverkehrsraum, Februar 2006.

Richtlinie 2014/92/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen (ABl Nr. L 257 v. 28.08.2014, S. 214).

Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36 EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl Nr. L 337 v. 23.12.2015, S. 35).

Richtlinie 2007/64/EG des Europäischen Parlaments und des Rats vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (ABl. L 319 v. 5.12.2007, S. 1).

Schweizerische Bankiervereinigung (SBVg), Positionspapier Payment Services Directive (PSD2), September 2017.

SEPA Data Model, Version 2.2., European Payments Council approved on 13 December 2006 (EPC029-06).

SEPA Instant Credit Transfer Scheem Rulebook, Version 1.1., European Payments Council approved on 18 October 2017 (EPC 004-16).

Verordnung (EG) Nr. 924/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über grenzüberschreitende Zahlungen in der Gemeinschaft und zur Aufhebung der Verordnung (EG) Nr. 2560/2001 (ABl. Nr. L 266 v. 09.10.2009, S. 11).

Verordnung (EG) Nr. 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers (ABl Nr. L 345 v. 8.12.2006, S. 1).

Verordnung (EG) Nr. 2560/2001 des Europäischen Parlaments und des Rates vom 19. Dezember 2001 über grenzüberschreitende Zahlungen in Euro (ABl Nr. L 344 v. 18.12.2001 S. 0013) (nicht mehr in Kraft).

Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (ABl Nr. L 123 v. 19.05.2015 S. 1).

Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl. Nr. L 94 v. 30.03.2012, S. 22).

(Starke) Kundenauthentifizierung: Aufsichtsrecht und Zivilrecht

Dr. Fabian Schmid, Zürich*

Inhaltsverzeichnis

* Dr. iur. Fabian Schmid, Leiter Regulatory & Compliance, BDO Financial Services, Zürich. Ich danke herzlich Frau Andrea Bigler, BLaw, und Herrn Anael Rosalen, BLaw, für die Unterstützung bei der Vorbereitung des Referats an der Schweizerischen Bankrechtstagung 2018 sowie bei der Verfassung dieses Beitrages.

I. Einleitung

Kundenauthentifizierung meint im Wesentlichen die Überprüfung der Identität und der Berechtigung des Kunden durch die Bank vor der Inanspruchnahme einer bestimmten Dienstleistung. In den letzten zwei Jahrzehnten haben sich bekanntlich elektronische Zahlungsdienstleistungen zu einem Massengeschäft entwickelt. Die meisten E-Banking-Kunden dürften die Erfahrung gemacht haben, dass die dabei zur Anwendung gelangten Authentifizierungsverfahren in der Praxis unterschiedlich ausgestaltet und zudem einem stetigen Wandel unterworfen sind. Im EU-Raum und selbstverständlich auch in der Schweiz wurde dieses Terrain bis vor kurzem noch kaum regulatorisch «besetzt».

Eine der wesentlichen Neuerungen der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt (Payment Services Directive, «PSD2») bildet nun die Einführung einer Pflicht für Zahlungsdienstleister zur Vornahme einer sogenannten starken Kundenauthentifizierung (auch: Strong Customer Authentication, «SCA»).[1]

Der Erlass der PSD2 als Ganzes wurde vom europäischen Gesetzgeber insbesondere auch mit der Notwendigkeit der Erhöhung des Konsumenten- bzw. Verbraucherschutzes angesichts erhöhter Risiken und fortschreitender

[1] Vgl. EUROPEAN PAYMENTS COUNCIL (EPC), PSD2 Explained, Infographic, June 2017.

technologischer Entwicklungen begründet.[2] So allgemein formuliert unterscheidet sich der Hauptzweck der PSD2 freilich noch kaum von den meisten anderen Regulierungsprojekten im Bereich des Finanzmarktrechts, deren ratio legis – auch in der Schweiz – üblicherweise mit der Erhöhung des Kunden- oder Anlegerschutzes begründet wird. In Bezug auf die Schaffung von Vorschriften zur starken Kundenauthentifizierung wird der Verbraucherschutzgedanke der PSD2 wie folgt näher konkretisiert: Einerseits soll durch die SCA der Schutz der beim Zahlungsdienstleister hinterlegten *Kundendaten* vor dem Zugriff durch unbefugte Dritte verbessert werden, andererseits soll sie den Schutz des Kunden vor *Betrug* im elektronischen Zahlungsverkehr erhöhen. Dass der letztgenannte Schutzzweck nicht nur im Interesse des Kunden, sondern angesichts der kundenfreundlichen Haftungsregelungen in der neuen PSD2 letztlich auch im Interesse der Banken liegt, versteht sich von selbst.

In Bezug auf den angestrebten erhöhten Schutz der Kunden vor Betrügern war sich der europäische Gesetzgeber durchaus bewusst, dass das Ziel einer vollständigen oder fast vollständigen Verhinderung von Betrugsfällen im Online-Banking rein illusorischer Art wäre. Beabsichtigt wird stattdessen eine «möglichst weitgehende Einschränkung des Betrugsrisikos»[3]. Tatsächlich bilden betrügerische Handlungen im elektronischen Zahlungsverkehr praktisch seit Beginn des Anbietens derartiger Dienstleistungen gegenüber Endkunden ein permanentes Übel. In der Schweiz wurden beispielsweise im Jahr 2016 insgesamt 824 Betrugsfälle von Trojanern im Bereich E-Banking gemeldet, wobei die Fallzahlen zuletzt stark schwankten.[4] Gemäss der schweizerischen Melde- und Analysestelle Informationssicherung (MELANI) würden Kriminelle zunehmend mobile Authentifizierungsmethoden beim E-Banking im Visier haben. Angriffe auf mobile E-Banking Systeme sollen sich häufen.[5]

---

2 Vgl. PSD2, Erwägungsgrund 7.

3 PSD2, Erwägungsgrund 95.

4 Vgl. Eidgenössisches Justiz- und Polizeidepartement (EJPD), Bundesamt für Polizei fedpol, Statistiken zum Jahresbericht 2017, abrufbar unter: <www.fedpol.admin.ch>.

5 Vgl. Melde- und Analysestelle Informationssicherung (MELANI), Newsletter vom 29. November 2016, abrufbar unter:<www.melani.admin.ch>; NZZ vom 30. November 2016 «Hacker attackieren Schweizer E-Banking Kunden».

II. Rechtsgrundlagen der starken Kundenauthentifizierung

1. PSD2

Die Grundzüge zur starken Kundenauthentifizierung werden neben den einschlägigen Definitionen von Art. 4 PSD2 primär in den Art. 97 und 98 PSD2 geregelt. Zudem stützen sich verschiedene Vorschriften der im Rahmen der PSD2 neu konzipierten Haftungsregelungen direkt auf die Vornahme bzw. das Unterlassen einer (ordnungsgemässen) starken Kundenauthentifizierung ab (Art. 72–74; 92 PSD2). Systematisch bilden die Bestimmungen damit Teil des Titels IV (Rechte und Pflichten bei der Erbringung von Zahlungsdiensten), welcher im Zusammenspiel mit Titel III (Transparenz der Vertragsbedingungen und Informationspflichten der Zahlungsdienste) gleichsam den «privatrechtlichen» Teil der PSD2 bildet.

Die Absätze 1, 2 und 4 von Art. 97 PSD2 definieren den sachlichen Anwendungsbereich der starken Kundenauthentifizierung und legen fest, wann diese – erweitert um das Element der so genannten dynamischen Verknüpfung – zu einer «qualifizierten starken Kundenauthentifizierung» wird.[6] Zudem werden den Zahlungsdienstleistern spezifische Pflichten zur Vornahme angemessener Sicherheitsvorkehrungen auferlegt (Abs. 2) und es wird das Verhältnis zwischen den Banken und den Drittanbietern im Sinne der PSD2, also den Zahlungsauslösedienstleistern und den Kontoinformationsdienstleistern, in Bezug auf die SCA geregelt (Abs. 5).

Art. 98 PSD2 delegiert die Ausarbeitung Technischer Regulierungsstandards zur starken Kundenauthentifizierung («RTS») an die Europäische Bankenaufsichtsbehörde EBA (in enger Zusammenarbeit mit der Europäischen Zentralbank EZB), wobei diverse materielle und formelle Vorgaben zu deren Ausarbeitung statuiert werden. Die Vorgaben an das Verfahren zur SCA, die Ausnahmetatbestände sowie die Anforderungen an die Sicherheitsmassnahmen sollen gestützt darauf auf Stufe Verordnung detailliert geregelt werden.

[6] Vgl. dazu Kap. III.5.

2. Technische Regulierungsstandards für SCA und Kommunikation (RTS)

Der finale Entwurf der Delegierten Verordnung (EU) zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation («RTS») wurde am 27. November 2017 durch die Europäische Kommission angenommen und publiziert. Hinsichtlich der SCA sind primär die ersten vier Kapitel (Art. 1–27 RTS) von Bedeutung. Die restlichen Bestimmungen der RTS (Art. 28–36) regeln die Anforderungen an die Kommunikation zwischen Zahlungsdienstleistern, Zahlern und Zahlungsempfängern im Sinne der PSD2; auf diese wird im vorliegenden Zusammenhang nicht näher eingegangen.

Die Zielsetzungen für die technischen Regulierungsstandards werden in Art. 98 Abs. 2 PSD2 festgehalten. Im Rahmen dieser Zielsetzungen stehen sich hinsichtlich der SCA im Wesentlichen zwei Interessensphären diametral gegenüber: einerseits das Interesse an erhöhter Sicherheit für die Kunden und andererseits das Bedürfnis der Kunden nach Wirtschaftlichkeit, Benutzerfreundlichkeit und Zugänglichkeit von elektronischen Zahlungsdienstleistungen. In diesem Spannungsfeld galt es bei der Ausarbeitung der RTS den richtigen Spagat zu finden. Ob dies gelungen ist, muss sich angesichts der noch bevorstehenden Umsetzung bzw. Implementierung der RTS in den europäischen Zahlungsverkehr noch zeigen.

3. Zeitplan

Die PSD2 bzw. deren nationale Umsetzungserlasse müssen von den Mitgliedstaaten grundsätzlich seit dem 13. Januar 2018 angewendet werden. Dies gilt für ausgewählte Vorschriften jedoch noch nicht, darunter auch jene zur SCA gemäss Art. 97 PSD2, welche erst 18 Monate nach dem Erlass der RTS eingehalten werden müssen.

Die Ratifizierung der RTS durch das EU-Parlament erfolgte am 13. März 2018, seither steht fest, dass die RTS (welche als Verordnung unmittelbar anwendbar sind und nicht in nationales Recht umgesetzt werden müssen) ab dem 14. September 2019 im gesamten EU-Raum einzuhalten sind.

III. Durchführung der SCA

1. Begriffsbestimmungen

Die Begriffe «Authentifizierung» sowie «starke Kundenauthentifizierung» werden in Art. 4 Ziff. 29 f. PSD2 definiert. Demnach handelt es sich bei der Authentifizierung um ein Verfahren, mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschliesslich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann.

Bei der starken Kundenauthentifizierung (Art 4 Ziff. 30 PSD2) handelt es sich darüber hinaus um eine Authentifizierung unter Heranziehung von mindestens zwei voneinander unabhängigen Elementen der Kategorien «Wissen» (etwas, das nur der Nutzer weiss), «Besitz» (etwas, das nur der Nutzer besitzt) oder «Inhärenz» (etwas, das der Nutzer ist), wobei diese Elemente insofern voneinander unabhängig sein müssen, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der andern nicht in Frage stellen darf. Zudem muss die SCA definitionsgemäss so konzipiert sein, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist. Auf diese Anforderungen ist nachfolgend näher einzugehen.

2. Elemente der (starken) Kundenauthentifizierung

Für Elemente aus der Kategorie *Besitz* kommen vorab so genannte Token in Betracht, also Geräte, die dem Kunden vom Zahlungsdienstleister bzw. von der Bank eigens für den Identifikations- und Authentifizierungsprozess abgegeben worden sind. Darüber hinaus fallen beispielsweise auch PC, Tablets oder Smartphones, sofern zum Empfang von Authentifizierungscodes geeignet, sowie Smartcards (Chipcards) in diese Kategorie.[7] Amtliche Ausweisdokumente hingegen dürften nicht in diese Kategorie gehören, da die Weitergabe solcher Dokumente an Dritte nicht verboten werden kann.[8] Die Umschreibung des Elements Besitz («etwas, das der Nutzer besitzt») wird in der Lehre zu Recht als unpräzise kritisiert. Eine Zahlungskarte beispielsweise kann ihre Eigenschaft als Authentifizierungselement nicht allein

[7] Vgl. Aufzählung bei BÖGER, Neue Rechtsregeln, S. 257.
[8] HOFFMANN, VuR 2016, S. 248.

deshalb verlieren, weil sie – ob willentlich oder unfreiwillig – in den Besitz eines anderen gelangt ist.[9] Andernfalls wäre eine SCA beispielsweise bei einem Missbrauch durch einen Dritten definitionsgemäss ausgeschlossen und die Haftungsregelungen wären hinfällig (aufgrund von Art. 74 Abs. 2 PSD2).

Als Elemente der Kategorie *Wissen* kommen etwa ein Passwort oder ein Code, eine PIN oder eine TAN in Betracht.[10] Unzulässig sind hingegen persönliche Daten, die grundsätzlich auch anderen Personen bekannt sind, wie etwa Name, Geburtsdatum, oder Adresse.[11] Ebensowenig dürfte die auf einer Zahlungskarte aufgedruckte Nummer, die jedermann wahrnehmen kann, den Anforderungen an die Kategorie Wissen genügen. Auch die Umschreibung des Elements Wissens («etwas, das der Nutzer weiss») fällt insofern zu restriktiv aus als beispielsweise eine PIN nicht allein schon deshalb ihren Status verliert, weil ein Dritter von ihr Kenntnis erlangt.[12]

Die Kategorie *Inhärenz* schliesslich beinhaltet menschlich-körperliche Merkmale, die sich unmittelbar auf den Nutzer beziehen und dessen zweifelsfreie Identifizierung ermöglichen. Beispiele hierfür sind Fingerabdruck, Stimme oder Gesicht des Kunden, also durchwegs Merkmale, welche sich heute mittels moderner Technologie, z.B. durch ein Smartphone bereitgestellt, rasch erkennen und zuordnen lassen.[13] In Bezug auf die Konkretisierung der Kategorie Inhärenz wird deutlich, dass es durchaus Elemente gibt, welche sich den drei Kategorien nicht eindeutig zuordnen lassen. Stellt eine Unterschrift beispielsweise etwas dar, das man weiss oder doch eher etwas, das man ist?

Für eine Qualifikation als starke Kundenauthentifizierung wird von der PSD2 lediglich verlangt, dass zwei Elemente der erwähnten drei Kategorien herangezogen werden, nicht jedoch, dass die betreffenden Elemente jeweils auch einer unterschiedlichen Kategorie angehören müssen.[14] Damit wird beispielsweise eine starke Authentifizierung anhand lediglich zweier Ele-

---

9 Hierzu und zum Folgenden: HOFFMANN, VuR 2016, S. 248.

10 Als Personal Identification Number (PIN) wird eine persönliche Identifikationsnummer bzw. eine Geheimzahl bezeichnet. Als Transaction Authentication Number (TAN) oder Transaktionsnummer gilt demgegenüber ein einmaliges Passwort zur Autorisierung einzelner Transaktion.

11 Vgl. BÖGER, Neue Rechtsregeln, S. 257.

12 HOFFMANN, VuR 2016, S. 248.

13 Vgl. EUROPEAN PAYMENTS COUNCIL (EPC), PSD2 Explained, Infographic, June 2017.

14 Hierzu und zum Folgenden: HOFFMANN, VuR 2016, S. 249.

mente aus der Kategorie Besitz bei Ausserachtlassung der übrigen Kategorien durch den Wortlaut der Richtlinie nicht per se ausgeschlossen. Genau zu prüfen wäre in diesem Fall jedoch das Erfordernis der Unabhängigkeit der Elemente.[15]

Die Art. 6 – 8 RTS konkretisieren die Anforderungen an die drei Elemente der SCA inhaltlich kaum, erweitern diese jedoch jeweils um aufsichtsrechtliche Aspekte. So wird darin festgehalten, dass die Zahlungsdienstleister spezifische Sicherheitsmassnahmen zu treffen haben zur Minderung des Risikos, dass die jeweiligen Elemente der SCA von Unbefugten verwendet, aufgedeckt oder offengelegt werden. Die Einhaltung der Sicherheitsmassnahmen zum Schutz der Vertraulichkeit der Authentifizierungsdaten ist zwingende Voraussetzung einer gültigen SCA.[16]

3. Unabhängigkeit der Elemente

Die für die SCA heranzuziehenden zwei Elemente aus den Kategorien Wissen, Besitz oder Inhärenz müssen gemäss Art. 4 Ziff. 29 PSD2 jeweils voneinander unabhängig sein. In Art. 9 RTS werden hierzu von den Zahlungsdienstleistern spezifische Massnahmen verlangt, die sicherstellen sollen, dass «hinsichtlich Technologie, Algorithmen und Parametern bei Verletzung eines der Elemente die Zuverlässigkeit der anderen Elemente nicht beeinträchtigt wird.» Letztlich geht es darum, dass die Überwindung des Schutzmechanismus, der auf einem Element beruht, nicht den auf dem anderen Element beruhenden Schutzmechanismus in Frage stellt.[17] Ein simples, wenn auch für bestimmte Authentifizierungsverfahren in der Praxis durchaus übliches Beispiel, in welchem gegen das Unabhängigkeitserfordernis der Elemente verstossen würde, wäre die Verwendung einer Zahlungskarte mit aufgedruckter Identifikationsnummer als einzige Elemente.

Fraglich ist das Zustandekommen einer gültigen SCA für den Fall, dass sämtliche verwendeten Elemente mit nur einem Gerät, z.B. einem Smartphone, verbunden sind (Mehrzweckgeräte). Konsequenterweise müsste das Erfordernis der Unabhängigkeit die Verwendung von Mehrzweckgeräten ausschliessen. Dennoch lassen die RTS Raum für die Verwendung von Mehrzweckgeräten für eine gültige SCA, allerdings sind dabei besondere

15 Zur Unabhängigkeit der Elemente siehe Kap. III.2.

16 Vgl. BÖGER, Neue Rechtsregeln, S. 257.

17 Hierzu und zum Folgenden: HOFFMANN, VuR 2016, S. 249.

Sicherheitsmassnahmen zum Schutz vor Missbrauch der Mehrzweckgeräte zu ergreifen (Art. 9 Abs. 2 und 3 RTS). Insbesondere sind gemäss den betreffenden Anforderungen an den Ausnahmetatbestand getrennte und sichere Ausführungsumgebungen durch die Software des Mehrzweckgeräts zu nutzen sowie Schutzmassnahmen zu ergreifen, dass die Software oder das Gerät nicht verändert werden.

4. Authentifizierungscode

Art. 4 Abs. 1 RTS wiederholt den in der PSD2 verankerten Grundsatz, wonach die Authentifizierung auf mindestens zwei Elementen der Kategorien Wissen, Besitz und Inhärenz zu basieren hat und fügt an, dass die Authentifizierung einen Authentifizierungscode nach sich ziehen muss. Dabei wird statuiert, dass der einzelne Authentifizierungscode vom Zahlungsdienstleister stets nur einmalig akzeptiert werden darf. Letzteres dürfte hierzulande im Rahmen der im Online-Banking zur Anwendung gelangenden Verfahren wie beispielsweise e-TAN, m-TAN oder PhotoTAN bereits seit längerer Zeit Standard sein.

In Art. 4 Abs. 2 und 3 RTS sind sodann diverse von den Zahlungsdienstleistern zu treffende Sicherheitsmassnahmen hinsichtlich der Generierung des Authentifizierungscodes sowie hinsichtlich der Vornahme der Authentifizierung mittels Authentifizierungscode verankert.

Die *Generierung* des Codes unterliegt spezifischen Sicherheitsmassnahmen, welche aufgrund des Gebots der Technologieneutralität, jedoch auf eher abstrakter Ebene gesetzlich umschrieben werden:

- aus der Offenlegung des Authentifizierungscodes dürfen keine Informationen über eines der drei Elemente der SCA abgeleitet werden können.
- Aufgrund der Kenntnis eines zuvor generierten Authentifizierungscodes darf kein neuer Authentifizierungscode generiert werden.
- Authentifizierungscodes dürfen nicht gefälscht werden können.

Hinsichtlich der *Vornahme* der Authentifizierung mittels Authentifizierungscode gelten sodann folgende Sicherheitsmassnahmen:

- Für den Fall, dass die Generierung eines Authentifizierungscodes fehlgeschlagen ist, darf nicht ermittelt werden können, welches der drei Elemente der SCA falsch war.

- Die Anzahl fehlgeschlagener Authentifizierungsversuche innerhalb einer bestimmten Zeitspanne darf nicht mehr als fünf betragen. Anschliessend erfolgt eine Sperrung.
- Die Kommunikationssitzungen sind gegen den Zugriff auf die während der Authentifizierung übertragenen Authentifizierungsdaten zu schützen.
- Die maximale Zeitspanne ohne Aktivität im Anschluss an die Authentifizierung darf nicht mehr als fünf Minuten betragen.

5. Dynamische Verknüpfung bei Auslösung elektronischer Zahlungsvorgänge

In bestimmten Anwendungsbereichen der SCA (dazu sogleich) genügt eine normale starke Kundenauthentifizierung nicht und es ist stattdessen zusätzlich eine so genannte *dynamische Verknüpfung* vorzunehmen (auch: qualifizierte starke Kundenauthentifizierung).[18] Dabei handelt es sich gemäss Art. 97 Abs. 2 PSD2 um eine starke Kundenauthentifizierung, welche Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten *Betrag* und einem bestimmten *Zahlungsempfänger* verknüpfen. Art. 5 RTS definiert die konkreten Anforderungen an eine SCA mit dynamischer Verknüpfung wie folgt:

- Zahlungsbetrag und Zahlungsempfänger werden dem Zahler angezeigt.
- Der generierte Authentifizierungscode gilt speziell für den Zahlungsbetrag und den Zahlungsempfänger, denen der Zahler beim Auslösen des Vorgangs zugestimmt hat.
- Der vom Zahlungsdienstleister akzeptierte Authentifizierungscode entspricht dem ursprünglichen spezifischen Zahlungsbetrag und der Identität des Zahlungsempfängers, denen der Zahler zugestimmt hat.
- Jede Änderung beim Betrag oder Zahlungsempfänger zieht die Ungültigkeit des generierten Authentifizierungscodes nach sich.

Da somit eine SCA mit dynamischer Verknüpfung jeweils die elektronische Generierung eines transaktions- und empfängerspezifischen Codes verlangt, ist klar, dass traditionelle Authentifizierungsverfahren wie TAN-Listen in

[18] So auch HOFFMANN, VuR 2016, S. 251.

Papierform, den neuen Anforderungen nicht mehr genügen.[19] Im Ergebnis führt das Erfordernis einer dynamischen Verknüpfung stattdessen zur zwingenden Verwendung von spezifisch generierten TANs.[20]

IV. Anwendungsbereich

Im Folgenden gilt es darzulegen, wann genau Zahlungsdienstleister eine SCA oder eine SCA mit dynamischer Verknüpfung durchzuführen haben. Hierzu ist zunächst von Art. 97 Abs. 1 PSD2 auszugehen, welcher diesbezüglich drei Fallgruppen skizziert. Danach hat ein Zahlungsdienstleister eine starke Kundenauthentifizierung durchzuführen, wenn der Zahler:

- online auf sein Zahlungskonto zugreift,
- einen elektronischen Zahlungsvorgang auslöst,
- über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

1. Online Zugriff auf ein Zahlungskonto

Von der Fallgruppe in Art. 97 Abs. 1 lit. a PSD2 («wenn der Zahler online auf sein Zahlungskonto zugreift») werden sämtliche Fälle erfasst, in welchen ein Kunde online auf sein Zahlungskonto zugreift, wobei die Auslösung eines Zahlungsvorganges nicht vorausgesetzt wird. Es genügt also für die Pflicht zur Vornahme seiner SCA grundsätzlich bereits, wenn der Kunde bloss seinen Kontostand via Online-Zugriff abfragen möchte.[21]

2. Auslösung elektronischer Zahlungsvorgänge

Der in Art. 97 Abs. 1 lit. b PSD2 definierte Anwendungsbereich der SCA («wenn der Zahler einen elektronischen Zahlungsvorgang auslöst») ist sehr weit gefasst. Neben sämtlichen Zahlungsaufträgen, welche ein Kunde über das Internet erteilt, inklusive Zahlungen im Rahmen des Online-Bankings,

19 Vgl. HOFFMANN, VuR 2016, S. 251.

20 BÖGER, Neue Rechtsregeln, S. 259.

21 Siehe auch BÖGER, Neue Rechtsregeln, S. 257. Vgl. aber die Ausnahmetatbestände in Kap. V.

gelten auch sämtliche stationäre Kartenzahlungen an Terminals (z.B. mittels EC-Karte) als elektronische Zahlungsvorgänge.[22]

Innerhalb dieser Fallgruppe wird indessen weiter differenziert. Gemäss Art. 97 Abs. 2 PSD2 ist nämlich bei «elektronischen *Fernzahlungsvorgängen*» eine starke Kundenauthentifizierung mit dynamischer Verknüpfung vorzunehmen, also eine qualifizierte starke Kundenauthentifizierung.[23] Als elektronische Fernzahlungsvorgänge gelten in diesem Zusammenhang sämtliche über das Internet ausgelösten Zahlungen einschliesslich des Online-Bankings sowie der Zahlungen, welche über elektronische Kommunikationsgeräte wie Mobiltelefone ausgelöst werden. Demgegenüber genügt bei Kartenzahlungen am Terminal des Zahlungsempfängers eine «normale» SCA.[24]

3. Handlungen mit Betrugs- oder Missbrauchsrisiko

Bei der in Art. 97 Abs. 1 lit. c PSD2 umschriebenen Fallgruppe («wenn der Zahler über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt») handelt es sich um einen sehr allgemein formulierten und daher schwer abgrenzbaren Auffangtatbestand, mit welchem generell alle Handlungen im Fernzugang erfasst werden sollen, die ein Betrugs- oder Missbrauchsrisiko beinhalten. Im Ergebnis führt dies dazu, dass die Zahlungsdienstleister im Zweifelsfall eine SCA durchführen sollten.[25]

V. Ausnahmen von der starken Kundenauthentifizierung

Art. 98 Abs. 1 lit. b PSD2 delegiert die Definition von Ausnahmen zum Anwendungsbereich der starken Kundenauthentifizierung an die EBA, setzt jedoch in Art. 98 Abs. 3 PSD2 die Leitplanken, welche für die Umschreibung der Ausnahmen zu berücksichtigen sind. Im Wesentlichen hatte die EBA bei der Definition des Ausnahmenkataloges in den RTS das mit der Dienstleistung verbundene Risikoniveau, den Betrag und/oder die Periodizität der

22 Dazu ausführlich HOFFMANN, VuR 2016, S. 251. Vgl. auch BÖGER, Neue Rechtsregeln, S. 258.

23 Dazu oben, Kap. III.5.

24 Dazu ausführlich HOFFMANN, VuR 2016, S. 252.

25 Vgl. BÖGER, Neue Rechtsregeln, S. 258.

Zahlung sowie den für die Ausführung des Zahlungsvorganges genutzten Zahlungsweg zu berücksichtigen.

Die EBA und gestützt auf deren Vorarbeiten die Europäische Kommission sind diesem Auftrag nachgekommen, indem in den Art. 10–18 RTS Ausnahmetatbestände definiert wurden, bei deren Erfüllung Zahlungsdienstleister keine SCA durchführen müssen. Besonderer Erwähnung verdienen hiervon insbesondere die folgenden Ausnahmetatbestände.[26]

1. Zahlungskontoinformation (Art. 10 RTS)

Beschränkt sich ein Online-Zugriff allein auf den Kontostand von zuvor genau zu diesem Zweck bezeichneten Konten oder werden lediglich Zahlungsvorgänge der letzten 90 Tage eingesehen, darf auf eine SCA verzichtet werden. Dabei dürfen allerdings keine sensiblen Zahlungsdaten offengelegt werden und die betreffende Ausnahme gilt nicht für einen erstmaligen Online-Zugriff. In diesem Zusammenhang dürfte beispielsweise das Abrufen des aktuellen Saldos mittels Smartphone-Applikation weiterhin ohne SCA möglich sein.

2. Vertrauenswürdige Empfänger (Art. 13 RTS)

Hat eine Kunde vorgängig und nach Anwendung einer SCA zuhanden des Zahlungsdienstleisters eine Liste mit vertrauenswürdigen (Zahlungs-) Empfängern definiert, so kann bei Überweisungen an die betreffenden Personen jeweils auf die Vornahme einer SCA verzichtet werden.

3. Wiederkehrende Zahlungen (Art. 14 RTS)

Für die Erstellung, Änderung oder erstmalige Auslösung einer Serie von ständig wiederkehrenden Zahlungsvorgängen mit demselben Betrag und demselben Zahlungsempfänger ist eine SCA vorzunehmen. Ist dies aber einmal erfolgt, muss nicht bei jedem einzelnen Zahlungsvorgang eine neue SCA durchgeführt werden. Ohne den betreffenden Ausnahmetatbestand würden Daueraufträge, wie beispielsweise jene zur Begleichung der monatlichen Mietzinsrechnungen, in der praktischen Handhabung stark eingeschränkt.

[26] Im Übrigen wird auf die Art. 10–18 RTS verwiesen.

4. Überweisungen zwischen Konten derselben Person (Art. 15)

Banken dürfen gestützt auf Art. 15 RTS auf die Vornahme einer SCA verzichten, wenn Zahler und Zahlungsempfänger identisch sind, d.h. wenn ein Kunde eine Zahlung an sich selbst als Empfänger in Auftrag gibt. Zusätzliches Erfordernis hierfür ist, dass sich beide Zahlungskonti bei derselben Bank befinden. Gestützt darauf dürften also beispielsweise im Online-Banking vorgenommene Kontoüberträge vom eigenen Privatkonto auf das eigene Sparkonto weiterhin ohne separate SCA möglich sein.

5. Kleinbetragszahlungen (Art. 16 RTS)

Beim Auslösen eines elektronischen Fernzahlungsvorgangs durch den Zahler dürfen Zahlungsdienstleister bis zu einem Betrag von maximal EUR 30 auf die SCA verzichten. Erforderlich ist jedoch, dass seit der letzten durchgeführten SCA der Totalbetrag aller ausgelösten Zahlungen nicht mehr als kumuliert EUR 100 beträgt oder dass seither nicht mehr als 5 einzelne Zahlungen vorgenommen wurden.

VI. Ausgewählte zivilrechtliche Aspekte im Zusammenhang mit der SCA

Durch die PSD2 wird das zivilrechtliche Verhältnis zwischen Zahler und Zahlungsdienstleister bzw. zwischen Kunde und Bank stark aufsichtsrechtlich überlagert. Im Sinne des vom europäischen Gesetzgeber angestrebten höheren Kundenschutzes resultierte daraus insgesamt eine Verlagerung der Haftung zugunsten der Kunden. Nachfolgend wird auf zentrale zivilrechtliche Regelungen der PSD2 eingegangen, welche direkt auf die Vornahme bzw. das Unterlassen einer (ordnungsgemässen) starken Kundenauthentifizierung abstützen.

1. Beweislast für Nachweis der erfolgten Authentifizierung

Für den Fall, dass ein Zahlungsdienstnutzer bestreitet, einen ausgeführten Zahlungsvorgang autorisiert zu haben, oder geltend macht, dass der Zahlungsvorgang nicht ordnungsgemäss ausgeführt wurde, trägt der Zahlungsdienstleister die Beweislast. In Anwendung von Art. 72 Ziff. 1 PSD2 muss er

insbesondere auch nachweisen, dass der Zahlungsvorgang authentifiziert war, er mithin eine gültige SCA vorgenommen hat.

2. Verschiebung der Haftungsverteilung bei unautorisierten Handlungen

Erfolgt ein nicht autorisierter Zahlungsvorgang, so hat der Zahlungsdienstleister nach Art. 73 Ziff. 1 PSD2 dem Zahler den Betrag unverzüglich, spätestens bis zum Ende des folgenden Geschäftstags, nachdem er von der unautorisierten Zahlung Kenntnis erhalten hat oder dieser ihm angezeigt wurde, zu erstatten. Ausgenommen sind diejenigen Fälle, in welchen der Zahlungsdienstleister berechtigte Gründe für den Verdacht, dass ein Betrug vorliegt, hat und der zuständigen nationalen Behörde die Gründe schriftlich mitteilt. Dem Zahlungsdienstleister obliegt es folglich, das belastete Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte.

Der Zahler kann nach Art. 74 Ziff. 1 PSD2 verpflichtet werden, infolge eines nicht autorisierten Zahlungsvorgangs unter Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder infolge der missbräuchlichen Verwendung eines Zahlungsinstruments entstehende Schäden zu tragen, jedoch bis maximal EUR 50. Von dieser Schadenstragungspflicht kann der Kunde aber wiederum entlastet werden, wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments für den Zahler nicht bemerkbar war oder der Verlust durch Handlungen bzw. Unterlassungen eines Angestellten oder Agenten, einer Zweigniederlassung eines Zahlungsdienstleisters oder einer Stelle, an welche die Tätigkeiten ausgelagert wurden, verursacht wurde.

Unabhängig vom genannten Höchstbetrag von EUR 50 hat der Zahler hingegen alle Verluste, die in Verbindung mit nicht autorisierten Zahlungsvorgängen entstanden sind, zu tragen, wenn er sie in betrügerischer Absicht oder durch vorsätzliche oder grob fahrlässige Verletzung seiner Pflichten nach Art. 69 PSD2 (Anzeigen von Verlust, Diebstahl, missbräuchlicher Verwendung oder nicht autorisierter Nutzung des Zahlungsinstruments; Treffen aller zumutbarer Vorkehrungen, um Sicherheitsmerkmale vor unbefugten Zugriff zu schützen) herbeigeführt hat.

Wird vom Zahlungsdienstleister des Zahlers hingegen keine starke Kundenauthentifizierung verlangt, so trägt der Zahler nach Art. 74 Ziff. 2 PSD2 einen finanziellen Verlust nur noch dann, wenn er in betrügerischer

Absicht gehandelt hat. In allen anderen Fällen, in denen der Zahlungsdienstleister des Zahlers keine SCA verlangt, trägt dieser den Schaden vollständig. Akzeptiert hingegen der Zahlungsempfänger oder der Zahlungsdienstleister des Zahlungsempfängers eine SCA nicht, so muss dieser den aus dem unautorisierten Zahlungsvorgang resultierenden Schaden tragen. Dabei kann sich der Kunde selbst dann auf den Ausschlusstatbestand von Art. 74 Ziff. 2 PSD2 berufen, wenn die SCA aufgrund einer Ausnahme nach Art. 98 PSD2 unterbleibt.[27]

Es bleibt anzumerken, dass diese Regelungen hinsichtlich der Haftungsverteilung finanzielle Anreize für die Zahlungsdienstleister schaffen, bei grösseren Zahlungen eine SCA zu verlangen.[28] Hingegen dürfte bei kleineren Zahlungen im Bereich der Ausnahmetatbestände das Interesse an der Benutzerfreundlichkeit tendenziell die Risiken überwiegen.

VII. Ausgewählte aufsichtsrechtliche Aspekte im Zusammenhang mit der SCA

Im Bereich der Vorschriften zur starken Kundenauthentifizierung, welche primär das Verhältnis zwischen Zahlungsdienstleister und Aufsichtsbehörde regeln, sind vorab die Vorschriften zur Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale hervorzuheben (Art. 97 Abs. 3 PDS2 i.V.m. Art. 22-27 RTS). Als personalisierte Sicherheitsmerkmale gelten jene Merkmale, die der Zahlungsdienstleister dem Kunden zum Zweck der Authentifizierung zur Verfügung stellt (z.B. PIN oder TAN), wobei im weiteren Sinne auch bereitgestellte Authentifizierungsgeräte und Software darunterfallen. Neben allgemeinen Anforderungen wie der Verpflichtung, die Vertraulichkeit und Integrität dieser Merkmale jederzeit zu gewährleisten (Art. 22 RTS) werden etwa auch detaillierte Vorgaben für die Erstellung und Übertragung der Sicherheitsmerkmale (Art. 23 RTS) oder deren Vernichtung und Widerruf (Art. 27 RTS) gemacht.

Eine nicht zu unterschätzende aufsichtsrechtliche Herausforderung dürfte für viele Zahlungsdienstleister die Umsetzung von Art. 2 RTS bilden, wonach sie über ein Transaktionsüberwachungssystem zur Erkennung nicht

[27] HOFFMANN, VuR 2016, S. 250.

[28] BÖGER, Neue Rechtsregeln, S. 260.

autorisierter oder betrügerischer Zahlungen verfügen müssen. In Ergänzung zur etablierten informatikgestützten Transaktionsüberwachung im Bereich der Geldwäschereibekämpfung muss hierzu eine zusätzliche Transaktionsüberwachung installiert oder ins bestehende System integriert werden. Diese dient jedoch nicht exakt demselben aufsichtsrechtlichen Ziel und muss daher mit abweichenden Parametern ausgestattet sein.

Erwähnenswert im Bereich der aufsichtsrechtlichen Aspekte der SCA sind schliesslich auch die Verpflichtung der Zahlungsdienstleister, die gesamten im Rahmen der RTS auferlegten Sicherheitsmassnahmen regelmässig von Prüfern «mit Fachwissen auf dem Gebiet der IT-Sicherheit und des Zahlungsverkehrs» prüfen zu lassen (Art. 3 RTS), ferner die Pflicht, SCA-spezifische Betrugsraten zu berechnen und Betrugsstatistiken zu erstellen (Art. 19 RTS) sowie die Verpflichtung zur umfassenden Sammlung und vierteljährlichen SCA-spezifischen Auswertung der Transaktionsdaten pro Zahlungsart (Art. 21 RTS).

VIII. Die SCA aus Schweizer Optik

Die Bedeutung der neuen Vorschriften zur SCA für Schweizer Banken ist vor dem Hintergrund der Frage zu beurteilen, welche Auswirkungen die PSD2 generell auf schweizerische Anbieter hat. Als EU-Richtlinie entfaltet diese in der Schweiz bekanntlich keine unmittelbaren rechtlichen Auswirkungen. Dennoch lassen sich mittelbare Auswirkungen nicht von der Hand weisen. Diese ergeben sich zunächst aufgrund der Anwendbarkeit der SEPA-Rulebooks, welche Schweizer Banken grösstenteils ratifiziert haben. Gestützt darauf werden die SEPA-Vertragsparteien dazu angehalten, den dritten und vierten Titel der PSD einzuhalten, deren Bestandteil auch die Vorschriften zur starken Kundenauthentifizierung bilden.[29]

Eine weitere mittelbare Anwendbarkeit kann sich aus dem zivilrechtlichen Cross-Border-Risiko ergeben, welches Banken mit einem signifikanten Anteil an Kunden aus dem EU-Raum tragen. Auf der Grundlage des Lugano-Übereinkommens (LugÜ) und der Rom I-Verordnung haben die betreffenden Kunden unter bestimmten Voraussetzungen die Möglichkeit, die

[29] SEPA Credit Transfer Scheme Rulebook, Rule 5.1; SEPA Direct Debit Scheme Rulebook Rule 5.1. Ausführlich zur Bedeutung der PSD 1 und PSD2 für Schweizer Banken vor dem Hintergrund der SEPA-Rulebooks: TRÜEB/KEISER, Regulierung und Marktzutritt, S. 175 ff.

Schweizer Bank auch in ihrem Domizilstaat zu beklagen, wobei das betreffende ausländische Recht zur Anwendung käme. Bei Rechtsstreitigkeiten im Bereich der Erbringung elektronischer Zahlungsdienstleistungen würde die Schweizer Bank in diesem Szenario auf Sorgfaltsstandards behaftet, welche den Vorgaben der PSD2 genügen müssen, namentlich auch den Vorgaben zur starken Kundenauthentifizierung.

Eine zusätzliche mögliche Implikation der PSD 2 besteht darin, dass die betreffenden Vorlagen, mangels vergleichbarer gesetzlicher Regelungen in der Schweiz, von hiesigen Zivilgerichten und Aufsichtsbehörden als Mindeststandards für die Beurteilung des erforderlichen Sorgfaltsmassstabes bei Zahlungsdienstleistungen verwendet würden. In Bezug auf die neuen Vorschriften zur starken Kundenauthentifizierung erscheint es durchaus realistisch, dass Schweizer Gerichte und Aufsichtsbehörden in der praktischen Rechtsanwendung zukünftig ein Sorgfaltsniveau voraussetzen dürften, welches dem im gesamten EU-Raum praktizierten Mindeststandard genügt.

Abschliessend stellt sich die Frage, ob in der Schweiz regulatorischer Handlungsbedarf hinsichtlich einer analogen Regulierung der elektronischen Zahlungsdienstleistungen besteht. Die Schweizerische Bankiervereinigung (SBVg) sprach sich in einem Positionspapier vom September 2017 dezidiert gegen eine derartige Notwendigkeit aus.[30] Sinngemäss wurde dabei auch argumentiert, dass das Sicherheitsniveau heute auf Eigeninitiative der Banken bereits auf einem sehr hohen Level sei, dass die Zwei-Faktor-Authentifizierung in der Schweiz heute bereits Standard sei und dass folglich kein Handlungsbedarf bestehe. Auch wenn dies insgesamt sicherlich zutrifft, so dürften heute wohl die wenigsten Schweizer Banken bereits Prozesse und Rahmenbedingungen implementiert haben, welche den Vorgaben zur starken (und qualifiziert starken) Kundenauthentifizierung gemäss PSD2 und RTS vollumfänglich entsprechen. Tatsache ist, dass in der Schweiz, abgesehen von allgemeinen aufsichtsrechtlichen Vorschriften, welche die Banken zum Schutz der Kundendaten verpflichten[31], der Authentifizierungsprozess zwischen Bank

30 SCHWEIZERISCHE BANKIERVEREINIGUNG (SBVG), Positionspapier Payment Services Directive (PSD2), September 2017. Vgl. aber TRÜEB/KEISER, Regulierung und Marktzutritt, S. 175 ff., welche von der Notwendigkeit der Einführung einer entsprechenden Regulierung in der Schweiz ausgehen.

31 Vgl. etwa FINMA-Rundschreiben 2008/21 Operationelle Risiken – Banken, Anhang 3 «Umgang mit elektronischen Kundendaten».

und Kunde weitgehend dem (allgemeinen) Privatrecht überlassen ist. Spätestens ab dem Inkrafttreten der RTS im September 2019 wird diesbezüglich gegenüber dem EU-Raum ein nicht unbedeutendes regulatorisches Gefälle bestehen. Dass daraus mittelfristig politischer Druck zur Angleichung der hiesigen Spielregeln resultieren könnte, kann zumindest nicht ausgeschlossen werden.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 30. April 2018.

BÖGER OLE, Neue Rechtsregeln für den Zahlungsverkehr – Zahlungskontengesetz und Zahlungsdiensterichtlinie II, in: Peter O. Mülbert, Volker Gross, Christian Grüneberg, Matthias Habersack, Rainer Metz (Hrsg.), Bankrechtstag 2016, Berlin, Frankfurt, Karlsruhe, München, Mainz 2016, S. 193–300.

HOFFMANN JOCHEN, Kundenhaftung unter der Neufassung der Zahlungsdiensterichtlinie, in: VuR 2016, S. 243–254.

TRÜEB HANS RUDOLF/KEISER BARBARA A., Regulierung und Marktzutritt dritter Zahlungsdienstleister, in: Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme / Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Zürich 2015, S. 161–180.

Unautorisierte Transaktionen im Zusammenhang mit Dritten Zahlungsdienstleistern

Susan Emmenegger*

Inhaltsverzeichnis

* Prof. Dr. iur., LL.M., ordentliche Professorin an der Universität Bern, Direktorin des Instituts für Bankrecht.

I. Dritte Zahlungdienstleister

Zu den zentralen Neuerungen der PSD2 gehört, dass sie ihren Anwendungsbereich auf sogenannte «dritte Zahlungsdienstleister» (ZDL) erweitert hat.[1] Dritte Zahlungsdienstleister erbringen kontobezogene, einen

[1] Im Hinblick auf die Zahlungsauslösedienste (ZADs) wurde dies auch von der EU-Kommission prominent in den Vordergrund gestellt, siehe den Vorschlag für eine Richtlinie, COM(2013) 547 final vom 24.07.2013, S. 8. Siehe auch Erw. 27 ff. PSD2 – Richtlinie (EU) 2015/2366 vom 25. November 2015 über Zahlungsdienste im Binnenmarkt [...] (ABl Nr. L 337 v. 23.12.2015, S. 35).

Zugriff auf das Konto voraussetzende Dienstleistungen, ohne dass sie dieses Konto selbst führen. Dritte Zahlungsdienstleister, die in der PSD2 geregelt sind, sind die Drittemittenten von Zahlungskarten, die Kontoinformationsdienste und die Zahlungsauslösedienste.

1. Drittemittenten von Zahlungskarten

Mit der Regelung von Drittemittenten von Zahlungskarten verfolgt die PSD2 das Ziel, das Angebot von Zahlungsinstrumenten zu erweitern.[2] Das Modell basiert auf den bestehenden Kreditkarten- bzw. Debitkarten-Schemes und soll insbesondere neuen Kartenanbietern den Marktzutritt ermöglichen. Bisher sind die Kartenherausgeber mit den Banken verbunden.[3] Mit der PSD soll der Markt auch für solche Drittemittenten geöffnet werden, die eigenständig agieren wollen. Es handelt sich um eine antizipierende Regulierung, bislang haben sich solche Akteure noch nicht etabliert.[4]

Weil die Drittemittenten Zahlungskarten ausgeben, ohne gleichzeitig das Konto des Zahlers zu führen, wird die Zahlung auch nicht direkt vom Konto des Zahlers abgebucht, sondern sie erfolgt zunächst durch den Drittemittenten selbst. Dieser verlangt dann einen Aufwendungsersatz vom Zahler. Der Aufwendungsersatz erfolgt durch die Einziehung des Betrages bei der Bank. Damit der Kartenemittent sicherstellen kann, dass eine Deckung vorhanden ist, muss er die Deckung bei der Bank abfragen können – und zwar auch dann, wenn er nicht schon (von vornherein) mit den Banken verbunden ist, wie das bei den traditionellen Kartenherausgebern (Visa, Mastercard) der Fall ist. Dieser Zugang auf das Kundenkonto wird ihm durch die PSD2 gewährt.[5]

---

2 Erw. 67 PSD2. Siehe hierzu auch TERLAU, ZBB 2/2016, S. 137.

3 In der Schweiz sind das z.B. Swisscard, Viseca Card Services, UBS Card Center und Cornèr Card. Siehe dazu und zur Funktionsweise von Zahlungskartensystemen STENGEL, Unautorisierte Transaktionen, S. 119 ff.

4 BÖGER, Neue Rechtsregeln, S. 282; SPINDLER/ZAHRTE, BKR 2014, S. 268. Die Irrelevanz der Dritten Zahlungsemittenten zeigt sich plastisch daran, dass sie – anders als die KIDs und die ZADs – noch nicht einmal über ein Akronym verfügen!

5 Art. 65 Abs. 1 PSD2.

2. Kontoinformationsdienste

Die PSD2 beschreibt die Kontoinformationsdienste (KIDs) als «Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält.»[6] Anders ausgedrückt bieten die Kontoinformationsdienste der Bankkundin einen Gesamtüberblick über ihre gesamten Kontobeziehungen, indem die Konten gebündelt dargestellt und meist auch mobil abgefragt werden können.[7] Diese Dienste werden regelmässig ergänzt durch weitere Dienstleistungen, z.B. Budgetierungstools oder Liquiditätspläne.[8]

Auch die Kontoinformationsdienste müssen für ihre Dienstleistung auf die Bankkonten ihrer Kundinnen zugreifen können. Mit Blick auf die Dienstleistung beschränkt sich der notwendige Zugriff allerdings auf den Informationsabruf.

3. Zahlungsauslösedienste

Zahlungsauslösedienste (ZADs) spielen insbesondere im Online-Handel eine Rolle. Sie schlagen eine Softwarebrücke zwischen der Webseite eines Online-Händlers und dem Webportal der Bank. Die Kundin autorisiert die Überweisung, indem sie in die Maske des Zahlungsauslösedienstes die entsprechenden Kontozugangsdaten eingibt. Die Daten des Händlers und der Betrag werden vom Dienstleister im Hintergrund hinzugefügt. In diesem Verfahren nimmt der Zahlungsauslösedienst die Zugangsdaten entgegen und leitet sie an die Hausbank weiter. Damit «löst» der Dienstleister den Zahlungsauftrag gegenüber der Bank aus. Sobald dies erfolgt ist, bestätigt er gegenüber dem Online-Händler, dass die Zahlung initiiert ist.[9]

---

6 Art. 4 Ziff. 16 PSD2.

7 Erw. 28 PSD2. Siehe auch LINARDATOS, WM Heft 7/2014, S. 300.

8 TRÜEB/KEISER, Dritte Zahlungsdienstleister, S. 166. Ein in der Schweiz aktiver Kontoinformationsdienstleister ist z.B. Qontis. In Deutschland ist es beispielsweise die «Star Finanz».

9 Beschreibung des Vorgangs bei BÖGER, Neue Rechtsregeln, S. 264. Detaillierte Beschreibung auch im Entscheid des deutschen Bundeskartellamtes zur Rechtswidrigkeit von Verboten in Bank-AGB betreffend die Weitergabe von Zugangsdaten an solche Dienstleister: BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 20.

So funktioniert beispielsweise die in der Schweiz tätige SOFORT GmbH.[10] Sie gehört seit 2014 zum Konzern der schwedischen Klarna-Bank und tritt heute vermehrt unter dem Namen bzw. Logo der Klarna auf. Andere Dienstleister hingegen beschränkten sich darauf, die Kundin von der Internetseite des Händlers in das Online-Banking seiner Hausbank weiterzuleiten; dort löst die Kundin dann selbst die Zahlung aus. Dieses System verwenden z.B. die Unternehmen giropay, iDeal, eps und Paydirekt.[11] Sie gelten unter der PSD2 nicht als Zahlungsauslösedienste.[12]

Welche Vorteile sind mit der Sofortüberweisung verbunden? Aus Sicht der Kundinnen fallen die Gebühren für die Kreditkartennutzung weg; die Direktüberweisungen per Zahlungsauslösedienst sind (bislang) kostenlos. Der Vorgang spart auch Aufwand, weil die Eingabe der Zahlungsdaten des Händlers automatisiert durch den ZAD eingefügt werden. Zudem spart die Kundin Zeit, denn der Händler erhält eine Echtzeitbestätigung des Überweisungsauftrags. Er kann daher die Bestellung sofort bearbeiten und die Ware direkt verschicken. Im Fall einer Online-Überweisung durch die Kundin würde die Zahlung regelmässig am nächsten Tag ausgelöst, dann muss sie beim Händler noch gutgeschrieben und der Zahlungseingang überprüft werden. Zwar könnte die Schweizer Kundin die Zahlung bis zu dessen effektiver Auslösung am Ende des Geschäftstages wieder stornieren.[13] Allerdings wird sie dies nicht wiederholt tun können, denn der Zahlungsdienstleister wird diese Information erhalten und diese Kundin sperren. Zudem setzt sich eine solche Kundin dem Betrugsvorwurf und dem Vorwurf der Leistungserschleichung aus. Kurz: die Risiken einer Stornierung halten sich in Grenzen.

---

10 Webseite: <www.sofort.de>.

11 Zu beiden Verfahren siehe TERLAU, jurisPR-BKR 2/2016, Anm. 1, S. 3. Zu Paydirekt BÖGER, Neue Rechtsregeln, S. 266. Beschreibung auch in BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 146 f.

12 TERLAU, jurisPR-BKR 2/2016 Anm. 1, S. 6.

13 Anders die Rechtslage in der EU. Gemäss Art. 80 PSD2 (früher: Art. 66 PSD1) kann der Zahler den Zahlungsauftrag nicht mehr widerrufen, sobald er beim Zahlungsdienstleister eingeht. Gemäss Art. 470 Abs. 2bis OR kann die Anweisung im zahlungslosen Bargeldverkehr nicht mehr widerrufen werden, sobald der Betrag dem Konto des Zahlers belastet ist. Die Belastung erfolgt in der Schweiz jeweils zum Tagesende (24 Uhr). Bis dann bleiben die Zahlungsaufträge pendent und können wieder gelöscht werden. Zur Rechtslage in Deutschland siehe etwa LINARDATOS, WM Heft 7/2014, S. 300.

Für den Händler liegt der Vorteil in der vergleichsweise geringen Gebühr, die er dem Zahlungsauslösedienst entrichten muss. Er weiss zudem dank der Echtzeitbestätigung des Transaktionsauftrags, dass der Zahlungsauftrag angenommen wurde und somit eine genügende Deckung besteht und dass auch keine anderen Hinderungsgründe für die Zahlungsausführung bestehen.[14] Insofern kommt der Vorgang einer Vorkasse (Vorauszahlung) nahe.[15] Die Echtzeitbestätigung bringt im Vergleich zur Vorkasse den Vorteil, dass der Händler den Verwaltungsaufwand zur Kontrolle des Zahlungseingangs spart und die Ware sofort versenden kann. Mit der schnellen Lieferung erreicht er eine grössere Kundenzufriedenheit. Schliesslich kann ein Online-Händler – etwa im Geschäft mit Online-Downloads oder Event-Tickets – auf diese Art auch neue Kundenkreise erschliessen, namentlich solche Kunden, die über keine Kreditkarte verfügen.[16] Zu denken ist angesichts der Beispiele vor allem auch an die jüngere Kundschaft.

II. Kritik an den Dritten Zahlungsdienstleistern

Im Zusammenhang mit den Dritten Zahlungsdienstleistern bestehen eine Reihe von Bedenken. Die Diskussionen beschränken sich auf die beiden Dienstleister, die bereits auf dem Markt tätig sind, also die Kontoinformationsdienste (KIDs) und die Zahlungsauslösedienste (ZADs). Unter den beiden Diensten sind die Bedenken zudem bei den Zahlungsauslösediensten besonders ausgeprägt – und zwar durchaus auch bei den Aufsichtsbehörden.[17]

1. Sicherheitsrisiken: Unautorisierte Transaktionen

Der am häufigsten genannte Kritikpunkt im Zusammenhang mit den Dritten Zahlungsdienstleistern ist das zusätzliche Sicherheitsrisiko. Denn

---

14 Siehe BÖGER, Neue Rechtsregeln, S. 264. Siehe auch BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 139. In der EU wird zudem der Zahlungsauftrag unwiderrufbar, er kommt daher einer Vorkasse nahe.

15 Allerdings kann die Schweizer Kundin den Auftrag noch bis zum Ende des Tages stornieren, siehe Fn. 13.

16 Erw. 29 PSD2. Siehe auch OMLOR, ZIP 12/2016, S. 561.

17 Siehe etwa den Fachartikel der deutschen BaFin aus dem Jahr 2014 (noch vor der definitiven Fassung der PSD2): BAFIN, Zahlungsdiensterichtlinie II: Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute.

aktuell erfolgt deren Kontozugriff standardmässig über Weitergabe der persönlichen Kontozugangsdaten, welche die Kundin den Dritten ZDL zur Verfügung stellt, indem sie diese auf deren Webportal in die dort vorgesehene Maske eingibt (sog. Screen Scraping). Darin wird ein erhöhtes Risiko für die Durchführung unautorisierte Transaktionen gesehen.

Im schweizerischen Recht ist die unautorisierte Transaktion nicht definiert. In Lehre und Rechtsprechung wird der Begriff des Legitimationsmangels verwendet. Damit sind aber regelmässig nur Zahlungen gemeint, bei denen der Zahlungsempfänger in betrügerischer Absicht gehandelt und eine unbefugte Zahlung an sich selbst bewirkt hat.[18] Die PSD2 fasst unter dem Begriff der unautorisierten Transaktion alle Zahlungen, die ohne Zustimmung des Zahlers erfolgen.[19] Der Begriff deckt also mehr als nur den Legitimationsmangel ab, er umfasst unter anderem auch die Doppelausführung oder versehentliche Ausführung von Überweisungen, die Vertretung ohne Vertretungsmacht, die Zahlung trotz Widerrufs, die Zahlung an einen falschen Empfänger wegen falscher IBAN-Angabe oder die mangelnde Geschäftsfähigkeit.[20]

Die hier angesprochenen Sicherheitsrisiken betreffen unautorisierte Transaktionen, bei denen sich betrügerisch handelnde Unbefugte Zugang zu einem fremden Konto verschaffen. Das sind im schweizerischen Verständnis die klassischen Legitimationsmängel.

a) Man-in-the-Middle-Angriffe

Bei den unbefugten Zugriffen auf die Bankkonten von Kundinnen, welche die Dienste von Dritten Zahlungsdienstleistern in Anspruch nehmen, steht nicht das Risiko im Vordergrund, dass der Dritte Zahlungsdienstleister den Kontozugang nutzen könnte, um selbst betrügerische Transaktionen zu seinen Gunsten zu tätigen. Diesbezüglich übt der Markt sowohl auf der Händler- als auch auf der Kundenseite eine genügende Kontrolle aus.

Im Zentrum der Sicherheitsdebatte stehen vielmehr die sogenannten «Man-in-the-Middle-Angriffe».[21] Bei solchen Angriffen schiebt sich der Angreifer (selbst oder über eine schädliche Software) zwischen die Kommuni-

---

18 Zu den verschiedenen Konstellationen siehe SCHALLER, Legitimationsmängel, S. 49 f.

19 Art. 64 Abs. 2 PSD2.

20 Beispiele bei BAUMBACH/HOPT HGB-HOPT, Bankgeschäfte, C/57.

21 Ausführlich dazu BAFIN, Zahlungsdiensterichtlinie II, Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute, S. 4 f.

kationspartner und leitet die Datenpakete auf ein drittes System um. Dabei spiegelt er den Kommunkationspartnern jeweils die Identität des anderen vor. Er kann die Datenpakete anschauen und verändern, bevor er sie an die Endstelle weiterleitet.[22] Der Angriff kann die Hardware jedes Kommunikationspartners (z.B. Computer, Handy), aber auch auf den Kommunikationsweg (WLAN, Angriff auf die HTTPS-Verbindung) gerichtet sein.

Bei der Einschaltung eines Dritten Zahlungsdienstleisters wird ein erhöhtes Risiko darin gesehen, dass es keine direkte Kommunikationslinie zwischen der Kundin und der Bank gibt, sondern dass sich andere Akteure dazwischenschieben. Damit werden zusätzliche Angriffspunkte für Man-in-th-Middle-Angriffe geschaffen.

b) Einschätzung des Risikos

Wie hoch ist das Risiko einer Man-in-the-Middle-Attacke im Falle der Nutzung eines Dritten Zahlungsdienstleisters, insbesondere eines Zahlungsauslösedienstes? Unstreitig schieben sich im Vergleich zu einem direkten Verbindungsaufbau zur kontoführenden Bank weitere Akteure in die Verbindung ein. Diese Akteure – also die Händler und insbesondere auch die Zahlungsauslösedienste – können selbst Zielscheibe eines Angriffs sein. Es entstehen also zusätzliche Angriffsstellen für Hacker-Angriffe.

Zu bedenken ist allerdings Folgendes: Der typische Risikofall bei Man-in-the-Middle-Angriffen ist der Angriff auf das IT-Umfeld der Bankkundin. Ein Angriff auf die Kunden-Hardware ist viel einfacher als ein Angriff auf die Sicherheitssysteme und die verschlüsselten Kommunikations-

---

[22] Siehe z.B. SCHAMAUN PHILIPP, Man-in-the-Middle-Angriffe (Stand: Dezember 2017), unter: www.sicherheitskultur.at/man_in_the_middle.htm. Siehe auch die Beschreibung bei BKartA-Beschl. B4-71/10 vom 29.06.2016, Rz. 53 Fn. 39: «Ziel eines Man-in-the-Middle-Angriffs ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer 'in die Mitte' der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf Antworten des Empfängers kann der Angreifer wiederum zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.».

kanäle von professionellen Marktteilnehmern. Der typische Man-in-the-Middle-Angriff verläuft dergestalt, dass der Angreifer der Kundin vorspiegelt, sie erhalte eine Kommunikation ihrer Bank. In diesem Zusammenhang wird die Kundin dann aufgefordert, eine Software herunterzuladen, die es dem Angreifer beim nächsten Zahlungsvorgang erlaubt, die Zugangsdaten abzufangen und die Zahlung zu manipulieren.[23] Oder aber die Kundin wird auf eine falsche Internetseite gelockt und dort aufgefordert, ihre Zugangsdaten einzugeben.[24]

Für einen Angreifer ist ein Angriff auf der Kundenseite auch deshalb viel einfacher als ein Angriff auf einen Zahlungsauslösedienst, weil er nur den Zahlungsvorgang einer einzigen Bank abbilden muss – er muss also nur wissen, wie das Login-Verfahren und die Zahlungsauslösung bei einer einzigen Bank funktioniert. Bei einem Angriff auf einen Zahlungsauslösedienst müsste er hingegen die Kommunikationsstruktur aller Banken nachbilden, was einen enormen Aufwand bedeuten würde. Hinzu kommt, dass Zahlungsauslösedienste im Zusammenhang mit dem Online-Handel zum Einsatz kommen. Die Kundin erwartet unmittelbar im Anschluss an die Zahlung eine Ware oder eine Dienstleistung. Das Zeitfenster für erfolgreiche Angriffe ist also deutlich kleiner als bei sonstigen Überweisungen.

Nach Angaben der hierzulande bekannten Klarna (früher: SOFORT GmbH) ist es seit der ersten Anwendung des Zahlungsverfahrens im Jahr 2005 im Rahmen der über 100 Millionen Transaktionen noch zu keinem Betrugsfall zu Lasten eines Kunden gekommen.[25] In einem Urteil des Oberlandesgerichts Frankfurt vom August 2016 heisst es, die Geltendmachung des Risikos einer Man-in-the-Middle-Attacke im Zusammenhang mit den Dienstleistungen der SOFORT GmbH bleibe «im abstrakten Bereich».[26]

---

23 So etwa der Sachverhalt in den Entscheiden des LG Darmstadt, siehe LG Darmstadt, Urteil vom 28. August 2014, 28 O 36/14 = WM 2014, S. 2323 ff.

24 So etwa der Sachverhalt im Entscheid des LG Köln, siehe LG Köln, Urteil vom 26. August 2014, 3O 390/13 = WM 2014, S. 2372 ff.

25 SCHOOR, Sofortüberweisung, S. 3. Siehe dazu OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016 = BKR 2017, S. 129 Rz. 40.

26 OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016 = BKR 2017 S. 129 Rz. 40. Der Streit handelte darüber, ob es zumutbar sei, wenn zur Erfüllung der gesetzlich geforderten kostenlosen Zahlungsmöglichkeit einzig die Zahlung über die SOFORT GmbH anbieten dürfe. Das OLG Frankfurt hat dies bejaht, der BGH hat dies im Rahmen der Anschlussberufung verneint. Zur Frage der Sicherheitsrisiken äusserte sich der BGH nicht. Siehe BGH, Urteil vom 18. Juli 2017 KZR 39/16 = NJW 2017, S. 3289. Unter der PSD2 hat sich die Frage erledigt.

c) Fazit

Insgesamt ist das erhöhte Risiko von Angriffen, insbesondere solchen, die eine unbefugte Zahlung auslösen würden, mehr gefühlter als tatsächlicher Natur. Nicht von der Hand zu weisen ist allerdings, dass die Nutzung von Zahlungsauslösediensten und überhaupt von Dritten Zahlungsdiensten dazu beiträgt, die Hemmschwelle für die Weitergabe von persönlichen Legitimationsmitteln (TAN[27], PIN[28]) herabzusetzen. Damit vergrössert sich mittelbar auch das Risiko, dass Unbefugte Kenntnis dieser Legitimationsmittel erhalten.

2. Datenschutz

a) Einblick in das Zahlungsprofil

Ein weiterer Kritikpunkt, der gegenüber den Dritten Zahlungsdienstleistern geäussert wird, betrifft den Datenschutz. Die Dritten Zahlungsdienstleister erhalten Zugriff auf die Kontodaten ihrer Nutzer. Im Falle von Kontoinformationsdienstleistern ergeben sich daraus sehr detaillierte Zahlungsprofile. Aber auch im Fall der Zahlungsauslösedienste besteht dieser Zugriff. Die in der Schweiz tätige Klarna (früher: SOFORT GmbH) weist denn auch ausdrücklich darauf hin, dass sie die Kontodeckung überprüft und die Überweisungen der letzten 30 Tage daraufhin untersucht, ob Überweisungen mit Klarna getätigt wurden. Tatsächlich erhalten Klarna und andere Zahlungsauslösedienste einen weit grösseren Zugriff; sie können die Zahlungshistorie soweit zurückverfolgen wie die Kundin selbst, und dies für alle Konten der Kundin bei der betroffenen Bank. Der Zugriff auf die gesamte Zahlungshistorie bzw. den kompletten Finanzstatuts der Kundin[29] erlaubt die Aus-

---

27 Transaction Number (Transaktionsnummer). TANs werden in verschiedenen Verfahren verwendet: Reguläre TAN: Man kann die TAN aus einer Liste auswählen (veraltet). Indizierte TAN (iTAN): Benutzer wählt eine vom Institut vorgegebene TAN aus einer TAN-Liste aus. Mobile TAN (mTAN): Dem Benutzer wird vor der Transaktion eine TAN als SMS übertragen. Smart TAN (sTAN): Erzeugung der TAN durch einen TAN-Generator. ChipTAN (chipTAN): Die TAN wird vom Institut als Balkencode übermitteld unt auf einem TAN-Generator angezeigt. Quelle: <https://www.itwissen.info/PIN-TAN-Verfahren-PIN-TAN-methode.html>.

28 Personal Identification Number (Persönliche Identifikationsnummer).

29 Gemäss der Stellungnahme der deutschen Kreditwirschaft wird diese Durchleuchtung bei einigen Dritten Zahlungsdienstleistern intensiv praktiziert, und zwar automatisiert und in Sekundenschnelle. Siehe DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 7.

wertung der Kontoinformationen für Bonitätsprüfungen oder für die Erstellung eines Verhaltensprofils, das dann selbst eingesetzt werden kann, etwa zur zielgerichteten Bewerbung von Finanzprodukten, oder an Dritte weiterveräussert werden kann.[30]

b) Einschätzung des Risikos

Unbestrittenermassen haben die Dritten Zahlungdienstleister Zugriff auf die Zahlungshistorien ihrer Nutzerinnen und Nutzern. Der Zugriff auf diese Daten erfolgt allerdings nicht unreguliert. Es gilt in der Schweiz das schweizerische Datenschutzgesetz, das den Dritten Zahlungsdienstleistern den Rahmen setzt. Das DSG gilt für die Dritten Zahlungsdienstleister genauso wie für die Banken. Letztere lassen sich im Rahmen der AGB durchweg ermächtigen, die im Rahmen ihrer Dienstleistung erlangten Daten über die Bankbeziehung(en) mit Kundinnen und Kunden für Marketingzwecke zu verwenden.

Hinzu kommt, dass die bislang in der Schweiz tätigen Dritten Zahlungsdienstleister entweder aus der Schweiz oder aus dem europäischen Ausland stammen. In Europa gilt ab dem 25. Mai 2018 die Datenschutzgrundverordnung, die deutlich strengere Anforderungen an die Datennutzung und Datenverarbeitung stellt als das schweizerische Datenschutzgesetz, und dies selbst bei Berücksichtigung der aktuellen Revision des DSG.

c) Fazit

Insgesamt hält sich im Zusammenhang mit den Dritten Zahlungsdienstleistern auch das *rechtliche* Risiko der Datensicherheit in Grenzen. Es ist denn auch weniger der rechtliche Rahmen, der in diesem Zusammenhang Probleme schafft, sondern vielmehr die Tatsache, das gewisse Nutzerinnen und Nutzer mit beachtlicher Leichtigkeit alle möglichen Zustimmungs-Buttons im Internet anklicken. Das ist allerdings ein generelles Problem, das nicht spezifisch mit dem Dienstleistungsangebot der Dritten Zahlungsdienstleister zusammenhängt.

---

30 SPINDLER/ZAHRTE, BKR 2014, S. 267 f. Siehe auch BÖGER, Neue Rechtsregeln, S. 267 m.w.N.

3. Wettbewerbsverzerrungen

Schliesslich wird geltend gemacht, dass Dritte Zahlungsdienstleister sich als Trittbrettfahrer betätigen, weil sie die von der Bank entwickelte und von ihr unterhaltende Online-Zahlungs- und Datenbankinfrastruktur, inklusive der kostenintensiven Sicherheitsstruktur, nutzen, ohne sich an den Kosten zu beteiligen.[31] Die Online-Händler sind nur deswegen bereit, für die Nutzung eines Zahlungsauslösedienstes ein Entgelt zu zahlen, weil sie eine Bestätigung über die tatsächliche Auftragsentgegennahme von der Bank erhalten. Für diese Dienstleistung bezahlen die Dritten Zahlungsdienstleister aber nichts.

Dieser Kritikpunkt lässt sich nicht abstreiten – im aktuellen System nutzen die Dritten Zahlungsdienstleister den Kontozugang, ohne dass die Bank dies erkennen kann. Insofern fehlt auch die Möglichkeit, eine Entgeltzahlung zu fordern.

Allerdings ist die Identifikation der Dritten Zahlungsdienstleister durch die Bank nicht zwingend mit einer Entgeltzahlung verbunden. Das zeigt sich am Regime der PSD2: Der Zugang der Dritten Zahlungdienstleister auf die Kundenkonten wird künftig über eine separate Schnittstelle erfolgen, so dass die Dritten Zahlungsdienstleister für die Bank erkennbar sind.[32] Die umfangreichen Kooperationspflichten der Bank sind aber gerade nicht an eine Entgeltzahlung gekoppelt; vielmehr bestehen die Kooperationspflichten der Bank unabhängig vom Bestand einer vertraglichen Beziehung zum Zahlungsauslösedienst.[33]

4. Fazit

An den Dritten Zahlungsdienstleistern wird regelmässig Kritik geübt. Im Vordergrund steht jeweils die Kritik bezüglich der fehlenden Datensicherheit und des fehlenden Datenschutzes. Diese Kritikpunkt halten einer näheren Betrachtung nur bedingt stand. Hingegen ist offensichtlich, dass die

---

31 Siehe dazu DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 6. Siehe auch BÖGER, Neue Rechtsregeln, S. 265.

32 Siehe Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23), Art. 30, 31. Zum Verbot des Screen Scraping siehe den ausdrücklichen Hinweis im Kommissionsentwurf C(2017) 7782 final S. 3. Siehe dazu auch hinten IV.3 (Marktzutritt zum Preis der Regulierung).

33 Art. 66 Abs. 5 PSD2.

Dritten Zahlungsdienstleister für ihre gewinnorientierten Dienste die Zahlungsinfrastruktur der Banken nutzen, ohne die Banken dafür zu entschädigen.

III. Haftung bei unautorisierten Transaktionen

Gemäss den obenstehenden Überlegungen besteht ein geringes Risiko, dass die Online-Verbindung der Kundin zu einem Dritten Zahlungsdienstleister für eine Hacking-Attacke genutzt wird. Dennoch soll hier solches Szenario im Hinblick auf die Schadens- bzw. Haftungsverteilung näher untersucht werden.

1. Beispiel: Man-in-the-Middle-Angriff auf den Zahlungsauslösedienst

Den Ausgang bildet folgendes Fallbeispiel: Eine Man-in-the-Middle-Attacke gegen einen Zahlungsauslösedienst ist erfolgreich verlaufen und ein falscher Zahlungsauslösedienst hat mithilfe der Zugangscodes, welchen die Kundin in die falsche Zahlungsmaske eingegeben hat, eine unautorisierte Zahlung ausgelöst. Die Kundin bemerkt die falsche Zahlung, weil die Ware nicht geliefert wird. Sie konsultiert online ihr Konto und stellt fest, dass eine Zahlung von CHF 3'000 an eine ihr unbekannte Gesellschaft in Georgien geleistet wurde. Sie beanstandet die falsche Belastung bei seiner Bank, erstattet Strafanzeige gegen Unbekannt und macht den fehlenden Betrag auch beim gehackten Zahlungsauslösedienst geltend. Die Frage ist, ob die Kundin die von ihr geltend gemachten Ansprüche erfolgreich durchsetzen kann.

2. Anspruch gegen die Bank

Gegenüber der Bank wird die Kundin einen Erstattungsanspruch geltend machen. Die Bank hat an einen Unbefugten geleistet. Entsprechend hat sie nicht gehörig erfüllt und ist zur Leistung nach wie vor verpflichtet.[34] Sie hat

[34] BGE 112 II 450 E. 4 S. 457; 132 III 450 E. 2 S. 452; BGer Urteil 4C.377/2000 vom 8. März 2001 E. 1b; 4C.28/2003 vom 15. Dezember 2003 E. 3.2.1; 4A_386/2016 vom 5. Dezember 2016 E. 2.2.2. Aus jüngerer Zeit zudem SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

aber ihrerseits einen verschuldensabhängigen Schadenersatzanspruch gegen die Kundin, falls diese am unbefugten Zahlungsvorgang ein Verschulden trifft.[35] Diese Regelung wird aber in den Banken-AGB durchweg modifiziert.

a) Legitimationsabrede

Die in der hier interessierenden Konstellation anwendbaren AGB zum Online-Banking sehen durchweg vor, dass Aufträge und Mitteilungen von Personen, die sich mit dem vorgesehenen Legitimationsverfahren Zugang zu den Online-Dienstleistungen der Bank verschaffen, als vom Kunden verfasst bzw. als von ihm autorisiert gelten und dass die Bank ermächtigt ist, diesen Instruktionen Folge zu leisten.[36]

Somit kann die Bank bereits gestützt auf die Legitimationsabrede geltend machen, dass sie keine Erstattungspflicht trifft. Ob die Legitimationsabrede vor einer gerichtlichen AGB-Kontrolle Bestand hat, wurde noch nicht getestet. Nach der hier vertretenen Auffassung verstösst sie gegen Art. 8 UWG. Denn eine Legitimationsabsprache, die selbst im Fall eines erfolgreichen Angriffs auf die Online-Banking-Systeme der Bank das Risiko auf die Kundin abwälzt, schafft ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und Pflichten im Bank/Kunden-verhältnis zum Nachteil der Konsumentinnen und Konsumenten.

Unter der Annahme, dass die AGB zum Online-Banking die Frage der Legitimationsmängel abschliessend regeln, führt der Verstoss der gängigen Legitimationsabsprache gegen Art. 8 UWG zum Fehlen einer AGB-Regelung. Es greift dann der Grundsatz, dass die Bank der Kundin den unbefugt abgebuchten Betrag wieder gutschreiben muss.

---

35 BGer 4A_438/2007 vom 29. Januar 2008 E. 5.1; SCHALLER, Legitimationsmängel, S. 46 f. m.w.N.

36 AGB-Beispiel: «Jede Person, die sich mit den persönlichen Legitimationsmitteln und dem in der «Anleitung» beschriebenen Legitimationsverfahren erfolgreich Zugang zu [Bank] Digital Banking verschafft (Selbstlegitimation), gilt der [Bank] gegenüber als zugriffsberechtigt; dies gilt unabhängig davon, ob es sich bei dieser Person tatsächlich um den Zugriffsberechtigten handelt bzw. diese vom Vertragspartner entsprechend autorisiert wurde. Sämtliche bei [Bank] über [Bank] Digital Banking eingehenden Weisungen und Instruktionen gelten als vom Zugriffsberechtigten verfasst. [Bank] gilt als beauftragt, im Rahmen des üblichen Geschäftsgangs diese Weisungen auszuführen sowie den Mitteilungen nachzukommen, sobald diesen eine korrekte Legitimationsprüfung zugrunde liegt.» (Stand: 1. Juni 2018).

b) Sorgfaltspflichten des Nutzers/der Nutzerin

Zwar hat die Bank nach dem Gesagten den Schaden aus einer unbefugten Zahlung selbst zu tragen. Sie hat aber ihrerseits einen Schadenersatzanspruch gegen die Kundin, falls diese an der unbefugten Zahlung ein Verschulden trifft.

Die AGB der Banken zu den Online-Dienstleistungen sehen vor, dass die Legitimationsmittel «keinesfalls weitergegeben oder in einer anderen Weise anderen Personen zugänglich gemacht werden» dürfen.[37] Zudem wird teilweise ausdrücklich erwähnt, dass die Anmeldung (das Login) immer nur auf der Bankseite erfolgen darf und nie auf der Drittseite eines Drittanbieters.[38] In diesem Zusammenhang wird dann auch ausgeführt, dass der Nutzer die Risiken trägt, die sich aus der Verletzung der genannten Sorgfaltspflichten ergeben.[39]

Die Nutzung von Zahlungsauslösediensten gilt mithin – falls sie nicht von der Bank anderweitig genehmigt wird – als Vertragsverletzung. Falls also der Zahlungsauslösedienst einer erfolgreichen Hacking-Attacke zum Opfer fällt, so liegt an deren Ursprung eine Vertragsverletzung durch die Kundin, für die sie sich nicht exkulpieren kann. Entsprechend kann die Bank den Schaden, den sie aufgrund einer unautorisierten Zahlung tragen muss, als Schadenersatz gestützt auf Art. 97 OR gegenüber der Kundin geltend machen. Ein Eigenverschulden der Bank wird man in diesem Fall nicht annehmen können. Also schuldet die Kundin den vollen Ersatz – im Ergebnis kann also die Bank den streitigen Betrag abbuchen.

c) Fazit

Resultiert im Zusammenhang mit der Nutzung eines Zahlungsauslösedienstes eine unautorisierte Abbuchung, so hat zwar die Bank diesen Schaden in einem ersten Schritt zu tragen. In einem zweiten Schritt kann sie

---

37 AGB-Beispiel: «Die Zugangsmittel (insbesondere PIN/Passwort, Sicherheitscode und Kartennummer oder Accesss Card) dürfen keinesfalls weiteregeben oder auf andere Weise anderen Personen zugänglich gemacht werden.».

38 Diese Klausel hat das deutsche Bundeskartellamt verboten, weil hierdurch ein Wettbewerbsnachteil zu anderen Zahlungdiensten entstehen würde. Siehe SCHOOR, Sofortüberweisung, S. 3. Siehe auch den Beschluss BKartA-Beschl. B4-71/10 vom 29.06.2016.

39 AGB-Beispiel: «Der Kunde/die Kundin trägt sämtliche Risiken, die sich aus der Preisgabe oder Aufzeichnung seiner/ihrer Legitimationsmittel ergeben.».

allerdings gegenüber der Kundin einen Schadenersatzanspruch aus Vertragsverletzung geltend machen (Art. 97 OR), denn die AGB untersagen es den Kundinnen und Kunden der Bank durchweg, ihre Legitimationsmittel an Dritte weiterzugeben oder sie auf einer anderen als der bankeigenen Webseite einzugeben.

3. Anspruch gegen den Zahlungsauslösedienst

Da bei der vorliegenden Konstellation der Zahlungsauslösedienst erfolgreich angegriffen wurde, liegt bei ihm auch der Ursprung für die unautorisierte Zahlung. Entsprechend stellt sich die Frage, ob die Kunding gegenüber dem ZAD einen Schadenersatzanspruch geltend machen kann.

a) Zahlungsauslösedienstleister als Beauftragter

Zwischen der Nutzerin und dem Zahlungsauslösedienstleister besteht nach schweizerischem Recht ein Auftragsverhältnis. Das verdient deshalb besondere Erwähnung, weil in Deutschland teilweise vertreten wird, es bestehe kein (Geschäftsbesorgungs-)Vertrag zwischen dem ZAD und dem Nutzer. Vielmehr handle sich um einen Vertrag zu Gunsten Dritter, der zwischen dem Händler und dem ZAD zugunsten des Nutzers geschlossen werde. Allerdings soll auch in dieser Konstellation ein Recht des Zahlers vereinbart sein, vom ZAD die Auslösung des Zahlungsvorgangs (direkt) zu fordern (§ 328 Abs. 1 BGB), und der ZAD wäre verpflichtet, sorgfältig mit den Zugangsdaten umzugehen.[40] Als Begründung für diese rechtliche Einordnung wird angeführt, dass die Zahlungsauslösung für den Kunden kostenlos sei. Zudem würden sich die ZAD selbst als Dienstleister des Händlers sehen.[41]

Aus schweizerischer Sicht ist die Rechtslage – jedenfalls im Hinblick auf die hier aktive Klarna (früher SOFORT GmbH) – anders zu beurteilen. Ein

---

40 TERLAU, jurisPR-BKR 2/2016, S. 11. Wohl befürwortend OLG Frankfurt, 11 U 123/15 (Kart) vom 24.08.2016, S. 9 («Soweit dieser Vertrag als Vertrag zu Gunsten Dritter im Sinne des § 328 BGB ausgestaltet sein dürfte ...»). Anders aber z.B. SPINDLER/ZAHRTE, BKR 2014, S. 269 (ausdrückliche Bezugnahme auf den «Vertrag» zwischen Zahler und TPP).

41 TERLAU, jurisPR-BKR 2/2016, S. 10, unter Hinweis auf die allgemeinen Geschäftsbedingungen der SOFRT GmbH bei Registrierung (der Händler) und die allgemeinen Geschäftsbedingungen eines Online-Händlers (OBI E-Commerce GmbH).

Vertrag kommt gemäss Art. 1 OR gestützt auf einen tatsächlichen oder rechtlichen Konsens zustande. Soweit hier ein tatsächlicher Konsens vom ZAD bestritten würde, wäre ein solcher gestützt auf das Vertrauensprinzip anzunehmen. Die Kundin wählt für den Zahlungsvorgang den ZAD. Dieser präsentiert sich ihr gegenüber als Dienstleister: Er stellt Masken zur Verfügung, welche die Kundin für den Bezahlvorgang nutzen kann. Gleichzeitig handelt es sich ersichtlich um einen unabhängigen Dritten und nicht um den Händler selbst. Die Kundin kann als vernünftige Person davon ausgehen, dass der ZAD ihm gegenüber eine Dienstleistung erbringt und über den entsprechenden Geschäfts- und Abschlusswillen[42] verfügt. Die Dienstleistung besteht – wie schon erwähnt – darin, dass der ZAD für die Kundin den Zahlungsvorgang erleichtert und anstösst, indem er als Erklärungsbote die Zahlung in Auftrag gibt. Dass kein separates Entgelt für die Dienstleistung des ZAD ausgewiesen ist, zerstört das Vertrauen über das Vorliegen eines Auftrags nicht, da das Obligationenrecht den Auftrag vermutungsweise als unentgeltliches Geschäft qualifiziert (Art. 394 Abs. 3 OR). Tatsächlich wird die Kundin nicht zu Unrecht davon ausgehen, dass solche Dienstleistungen vom Händler gesamthaft eingepreist sind.

Hinzu kommt, dass – jedenfalls im Fall der Klarna – im Rahmen der FAQ die Dienstleistung gegenüber der Kundin konkretisiert wird. Dort werden unter dem Titel «Unser Versprechen», verschiedene Zusicherungen gemacht. Die wichtigste Zusicherung besteht in der «Verpflichtung» (*sic*) einer Schadensfreistellung im Fall des Datenmissbrauchs (dazu unten). Diese Versprechen richten sich, da sie auf der Seite des Zahlvorgangs erscheinen, zwangsläufig an die Nutzerin dieses Dienstes. Wer in dieser Weise etwas verspricht, gibt einen vertraglichen Bindungswillen kund – tatsächlich, mindestens aber vertrauenstheoretisch.

Schliesslich scheint auch die PSD2 als «Geburtshelferin» der Dritten Zahlungsdienstleister von einer vertraglichen Rechtsbeziehung zwischen dem ZAD und den Nutzerinnen und Nutzern auszugehen; sie definiert den Zahlungsauslösedienst als Dienst, der «auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag.... auslöst.»[43] Zudem spricht sie vom «Vertrag zwischen dem Zahler und dem Zahlungsauslösedienstleister» (Art. 73 Abs. 3 PSD2).

---

42 Siehe hierzu GAUCH/SCHLUEP/SCHMID/EMMENEGGER, OR AT I, Rn. 171, Rn. 308.

43 Art. 4 Ziff. 15 PSD2.

Im Ergebnis besteht zwischen dem ZAD und der Kundin ein Auftragsverhältnis im Sinne von Art. 398 ff. OR.

b) Schadensfreistellung in den AGB

Im Fall der in der Schweiz tätigen Klarna richtet sich der Schadenersatzanspruch zunächst nach der vertraglichen Vereinbarung zwischen ihr und der Kundin. Die Klarna sichert unter der Sparte FAQ «Unser Versprechen» den Zahlern eine «Schadensfreistellung für den unwahrscheinlichen Fall eines Datenmissbrauchs» zu.[44] Wörtlich heisst es, dass sich die Sofort GmbH verpflichtet, den «Endkunden, die PIN und TAN in unser System eingeben, von etwaigen Vermögensschäden freizustellen, die dem Endkunden möglicherweise dadurch entstehen, dass seine über unser System geroutete PIN- und TAN-Daten missbraucht werden und dem Endkunden durch die Verwendung der über unser System gerouteten PIN und TAN ein Schaden entsteht.»[45] Der Freistellungsanspruch ist betraglich nicht limitiert; eine Begrenzung ergibt sich aus dem Kausalzusammenhang zwischen der missbräuchlichen Verwendung der Zugangsdaten und dem Schaden.

Dass im Falle einer Man-in-the-Middle-Attacke die Zugangsdaten nicht über das System der Sofort GmbH geroutet werden, weil sie vorher abgefangen und umgeleitet werden, steht dem Freistellungsanspruch nicht entgegen. Nach dem Vertrauensprinzip liegt darin eine umfassende Schadensfreistellung für Datenmissbrauch im Einflussbereich des Zahlungsauslösedienstes.

c) Haftung aus Auftragsrecht

Andere Zahlungauslösedienste können andere AGB enthalten oder den Fall der Legitimationsmängel gar nicht regeln. Dann kommt als Auffangordnung das Auftragsrecht zur Anwendung. Danach haftet der ZAD der Kundin für die getreue und sorgfältige Ausführung des ihm übertragenen Geschäfts (Art. 398 Abs. 2 OR). Gelingt es einem Angreifer, den ZAD erfolgreich zu hacken und sich als Man-in-the-Middle zwischen den ZAD und den Kunden zu stellen und so den Datenzugang abzufangen, so ist auf eine Sicherheitslücke beim ZAD zu schliessen. Dass diese auf die Unsorgfalt des ZAD

---

44 FAQ Sofort GmbH, auch einsehbar bei der Demo-Version:< https://www.sofort.com/payment/multipay/go/login>.

45 *Id.*

zurückgeht, muss der Kunde nachweisen. An den Nachweis sind aber keine hohen Anforderungen zu stellen – zumal etwa im Fall der Klarna der ZAD damit wirbt, zu den sichersten Bezahlverfahren weltweit zu gehören. Das fehlende Verschulden ist sodann vom ZAD nachzuweisen. Die Umstossung der Vermutung dürfte ihm aber kaum gelingen.

d) Fazit

Wird der Zahlungsauslösedienst erfolgreich gehackt, führt dies zu einem Schadenersatz seitens der Kundin. Die in der Schweiz tätige Klarna verpflichtet sich sodann gegenüber dem Nutzer zur unlimitierten Schadensfreistellung für den Fall eines Datenmissbrauchs in ihrem Einflussbereich. Für das hier gewählte Szenario einer erfolgreichen Man-in-the-Middle-Attacke auf den ZAD bedeutet dies, dass der ZAD der Kundin den aus dem Datenmissbrauch entstandenen Schaden ersetzen wird.

4. Ergebnis

Im Ergebnis muss also die Kundin gegenüber der Bank einen ZAD-relevanten Schaden tragen, aber sie hat gegenüber dem ZAD gestützt auf dispositives Gesetzesrecht oder einzelfallsweise gestützt auf die vertragliche Vereinbarung einen Anspruch auf Schadenersatz. Das erscheint sachgerecht, es blendet allerdings eine Schwierigkeit aus: Wenn das Konto der Kundin aufgrund eines betrügerischen Eingriffs belastet wird, so ist es für die Kundin sehr schwer erkennbar, wo der Angriff stattgefunden hat. Dies umso mehr, als die Kundin zwar gegenüber ihren Beauftragten (Bank, ZAD) Informationsansprüche hat und diese ihr Rechenschaft über den ordnungsgemässen Zahlungsablauf schulden. Aber diese Pflichterfüllung muss die Kundin zunächst geltend machen und allenfalls gerichtlich einklagen.

IV. Haftungsregelung unter der PSD2

Es wurde bereits darauf hingewiesen, dass die Aufnahme der Dritten Zahlungsdienstleister in den Anwendungsbereich der PSD2 zu den Hauptpunkten der Revision gehörten. Zu den Regelungspunkten zählen selbstredend auch die Haftungsfragen im Zusammenhang mit einem möglichen Datenmissbrauch, der zu einer unautorisierten Transaktion führt. Die Haftungsfrage ist aber eingebettet in einen generellen Regulierungsrahmen, der im Blick bleiben muss, wenn man die Haftunsfragen genauer anschaut.

1. Unterscheidung zwischen Aussen- und Innenverhältnis

a) Aussenverhältnis: Erstattungspflicht der Bank

Erfolgt im Zuge der Nutzung eines Zahlungsauslösedienstes eine unautorisierte Zahlung, so sind aus der Sicht der Kundin zwei Dienstleister involviert und zwei Fehlerquellen möglich: Die Bank und der Zahlungsauslösedienst. Die aus schweizerischer Sicht bestehende Schwierigkeit für die Kundin, die Fehlerquelle zu identifizieren, wird in der PSD2 mit einer wichtigen Weichenstellung ausgebügelt. Gegenüber der Kundin ist allein die Bank die Ansprechpartnerin. Sie haftet für Legitimationsmängel in gleicher Weise, wie wenn kein Dritter Zahlungsdienstleister an der Transaktion beteiligt gewesen wäre. Es gilt also das reguläre Haftungsregime der PSD2:[46] Bei einer Zahlung an einen Unbefugten hat die Kundin einen unverzüglichen Erstattungsanspruch gegenüber der Bank.[47] Die Bank hat ihrerseits für den Schaden, der ihr aufgrund der unverzüglichen Erstattungspflicht entsteht, grundsätzlich einen Schadenersatzanspruch gegenüber der Kundin. Dieser ist stufenweise geregelt:

- Die Kundin haftet voll, wenn sie in betrügerischer Absicht gehandelt hat.[48]
- Die Kundin haftet voll, wenn sie grobfahrlässig ihre Sicherungs- und Anzeigepflichten verletzt hat.[49] Allerdings verliert die Bank selbst in diesem Fall ihren Schadenersatzanspruch, wenn sie ihrerseits keine starke Kundenauthentifizierung verlangt hat.[50]

---

46 Art. 73, 74 PSD2. Siehe dazu EMMENEGGER, Eckpunkte, S. 53 ff.

47 Art. 73 Abs. 2 PSD2 hält die unverzügliche Erstattungspflicht der Bank für Zahlungen unter Nutzung eines ZAD ausdrücklich fest. Die Erstattung hat bis zum nächsten Geschäftstag zu erfolgen. Eine Ausnahme gilt, wenn die Bank berechtigte Gründe für den Verdacht hat, dass seitens der Kundin ein Betrug vorliegt. Selbst in diesem Fall darf sie die Gutschrift nur verweigern, wenn sie der Behörde eine entsprechende Meldung erstattet (Art. 73 Abs. 1 PSD2).

48 Art. 74 Abs. 1. Dabei gilt als Beweislastregel, dass die ordnungsgemässe Authetifizierung und die ordnungsgemässe Aufzeichnung des Zahlungsvorgangs nicht genügt, um der Kundin eine betrügerische Absicht zu unterstellen. Die PSD2 hält weitergehend fest, dass die Bank «unterstützende Beweismittel» vorlegen muss, wenn sie den Betrug der Kundin nachweisen will, Art. 72 Abs. 2 PSD2.

49 Art. 74 Abs. 1 Unterabsatz 3.

50 Art. 74 Abs. 2 PSD2. Zur starken Kundenauthentifizierung siehe SCHMID, (Starke) Kundenauthentifizierung, passim.

- Die Kundin haftet mit einem Höchstbetrag von 50 Euro, wenn sie an der unautorisierten Zahlung ein leichtes Verschulden trifft.[51]
- Trifft die Kundin kein Verschulden, so enfällt der Schadenersatzanspruch der Bank. [52]

b) Innenverhältnis: Regressansprüche gegen den Zahlungsauslösedienst

Die Bank trifft im Fall der Zahlung an einen Unbefugten gegenüber dem Kunden zwar auch dann eine unverzügliche Erstattungspflicht, wenn ein Zahlungsauslösedienst genutzt wurde. Hingegen kann sie im Innenverhältnis auf den Zahlungsauslösedienst Regress nehmen, wenn der Fehler in der Ausführung des Zahlungsvorgangs in dessen Verantwortungsbereich fällt.[53] Es gibt also für die Bank eine Möglichkeit der Schadensabwälzung; allerdings trägt sich im Innenverhältnis nach wie vor das Insolvenzrisiko des Zahlungsauslösedienstes.[54] Dieses Risiko ist zwar durch die Versicherungspflicht des Zahlungsauslösedienst reduziert,[55] aber nicht völlig ausgeschlossen.

Im Falle eines Regressanspruchs der Bank muss der Zahlungsauslösedienst nachweisen, dass der Zahlungsvorgang ordnungsgemäss ausgeführt wurde. Das bedeutet konkret: Der Zahlungsauslösedienst muss nachweisen, dass der Zahlungsvorgang innerhalb seines Zuständigkeitsbereichs authentifiziert, ordnungsgemäss aufgezeichnet und nicht durch eine technische Panne oder einen anderen Mangel im Zusammenhang mit seiner Dienstleistung beeinträchtigt wurde.[56] Der Zahlungsauslösedienst hat also einen Anreiz, seine Tätigkeit zu dokumentieren, um sich gegen mögliche Regressansprüche der Bank zu wappnen. Damit erhöht sich auch die Sicherheit seiner Prozesse, und damit die Sicherheit des Zahlungsverkehrs allgemein.[57]

---

51 Art. 74 Abs. 1 PSD2.

52 Art. 74 Abs. 1 lit. a PSD2: «wenn der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments für den Zahler vor einer Zahlung *nicht bemerkbar* war, es sei denn, der Zahler hat selbst in betrügerischer Absicht gehandelt.».

53 Art. 73 Abs. 2 Unterabs. 2 PSD2; Erw. 73 PSD2.

54 OMLOR, ZIP 12/2016, S. 562; BÖGER, Neue Rechtsregeln, S. 277.

55 Art. 5 Abs. 2 PSD2.

56 Art. 73 Abs. 2 Unterabs. 2 PSD2.

57 BÖGER, Neue Rechtsregeln, S. 277.

c) Weitergehende Ansprüche der Kundin

Die Richtlinie regelt lediglich den Erstattungsanspruch der Kundin für Zahlungen an Unbefugte. Für weitere Schadenersatzansprüche, etwa für Folgeschäden oder sonstige mittelbare Beeinträchtigungen, verweist sie auf das anwendbare nationale Vertragsrecht.[58] Dabei wird ausdrücklich auf den Vertrag der Kundin mit der Bank, aber auch auf den Vertrag der Kundin mit dem Zahlungsauslösedienst verwiesen.

In der Doktrin wird diese Regelung dahingehend interpretiert, dass die Kundin gegenüber dem Zahlungsauslösedienst nicht nur Schadenersatzposten geltend machen kann, die über die Erstattungspflicht der Bank hinausgehen, sondern dass sie auch für den fehlenden Kontobetrag einen direkten Anspruch gegenüber dem Zahlungsauslösedienst hat.[59] Die praktische Bedeutung dürfte allerdings gering sein, da es einfacher sein dürfte, den Erstattungsanspruch gegen die kontoführende Hausbank durchzusetzen, die sich meist auch in geographischer Nähe der Kundin befindet.

2. Entlastung der Banken durch Abschottung?

a) Ausdrückliche Erlaubnis der Nutzung von Zahlungsauslösediensten

Angesichts der strengen Haftungsregelung für die Banken, die in einem ersten Zugriff sämtliche Risiken für unautorisierte Zahlungen tragen müssen, wäre es naheliegend, dass die Banken die Nutzung von Zahlungsauslösediensten möglichst zu verhindern suchen. Gerade dies lässt aber die Richtlinie nicht zu. Die PSD2 hält ausdrücklich fest, dass die Nutzung von Zahlungsauslösediensten unter Verwendung der personalisierten Sicherheitsmerkmale zulässig ist.[60] Die AGB der EU-Banken enthielten bis anhin Sorgfaltspflichten und Weitergabeverbote, wie sie auch heute noch in den AGB der Schweizer Banken zu finden sind. Unter der PSD2 sind solche Weitergabeverbote im Hinblick auf die Dritten Zahlungsdienstleister nicht mehr zulässig.[61]

---

58 Art. 73 Abs. 3 PSD2.

59 BÖGER, Neue Rechtsregeln, S. 276.

60 Art. 66 Abs. 1 und 3 lit. b PSD2; Erw. 69 und 96 PSD2.

61 LINARDATOS, WM Heft 7/2014, S. 301; BÖGER, Neue Rechtsregeln, S. 272.

b) Ausdrückliche Kooperationspflicht der Banken

Angesichts der ablehenden Haltung der Kreditindustrie im Hinblick auf die Dritten Zahlungsdienstleister[62] sah sich der Richtliniengesetzgeber zudem zur ausdrücklichen Statuierung von Kooperationspflichten seitens der Banken gegenüber den Dritten Zahlungsdienstleistern veranlasst. Die Banken sind verpflichtet, Zahlungen, die über Zahlungsauslösedienste angestossen werden, gleich schnell und zu denselben Kosten («ohne Benachteiligung») auszuführen,[63] und dem Zahlungsauslösedienst alle Informationen zugänglich zu machen, über welche die Bank selbst verfügt.[64] Damit wird unter anderem gewährleistet, dass die Online-Händler auch bei Nutzung des Zahlungsauslösedienstes eine verlässliche Echtzeit-Bestätigung über den Zahlungsauftrag erhalten.[65] Die Verweigerung der Kooperationspflicht ist nur möglich bei betrügerischen oder nicht autorisierten Zugängen zum Bankkonto. Allerdings müssen dafür objektive und gebührend nachgewiesene Gründe bestehen; sodann ist der Zahler grundsätzlich unverzüglich nach der Verweigerung darüber in Kenntnis zu setzen.[66]

Die Kooperationspflichten der Bank sind zudem gemäss Richtlinie unabhängig vom Bestand einer vertraglichen Beziehung zum Zahlungsauslösedienst.[67] Das bedeutet gleichzeitig, dass die Kooperationspflicht nicht von der Zahlung eines Entgelts seitens des Zahlungsauslösedienstes abhängt.[68] Diesbezüglich hat also die Richtlinie eine Weichenstellung vorgenommen, die der Kritik der Banken an der Trittbrettfahrer-Rolle der Dritten Zahlungsdienstleister keine Rechnung trägt.

Schliesslich ist in diesem Zusammenhang noch zu erwähnen, dass der Zahlungsauslösedienst die Authentifizierungsverfahren nutzen darf, welche die Bank für ihre Kunden verwendet.[69] Die Richtlinie stellt damit sicher, dass die Kundinnen und Kunden trotz Nutzung eines ZAD keine zusätzlichen Sicherheitsmerkmale eingeben müssen, was den Aufwand erhöht und als Marktzugangsbarriere gewirkt hätte.[70]

---

62 Siehe etwa DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme, S. 4 f.
63 Art. 66 Abs. 4 lit. c PSD2. Siehe auch Art. 66 Abs. 2 PSD2.
64 Art. 66 Abs. 4 lit. b PSD2.
65 BÖGER, Neue Rechtsregeln, S. 272.
66 Art. 68 Abs. 5 PSD2.
67 Art. 66 Abs. 5 PSD2.
68 BÖGER, Neue Rechtsregeln, S. 272.
69 Art. 97 Abs. 5 PSD2.
70 BÖGER, Neue Rechtsregeln, S. 278.

3. Marktzutritt zum Preis der Regulierung

Der forcierte Marktzugang der Dritten Zahlungsdienstleister und insbesondere der Zahlungsauslösedienste ist allerdings auch für diese Dienste nicht umsonst zu haben. Sie werden insgesamt in den Regelungsrahmen der PSD2 eingebunden und für sie gilt ein umfangreiches Pflichtenheft. Tatsächlich wird auch in den Erwägungen zur PSD2 als wesentliche Zielsetzung der Richtlinie die Schaffung von klaren Regelungen für Dritte Zahlungsdienstleister, insbesondere auch im Hinblick auf den Daten- und den Verbraucherschutz, definiert.[71]

a) Bewilligungspflicht und laufende Überwachung

Zunächst einmal führt die PSD2 für die Dritten Zahlungsauslösedienste eine Bewilligungspflicht ein und unterstellt sie einer laufenden Überwachung.[72] Kontoinformationsdienste unterstehen einer Registrierungspflicht.[73] Damit wird erstens einem Wildwuchs von zweifelhaften Anbietern mit zweifelhaften Geschäftsmodellen ein Riegel geschoben. Die Eckpunkte der Zulassungsbedingungen für die ZADs unterscheiden sich nicht stark von den Bewilligungsvoraussetzungen nach dem BankG/FINIG, allerdings sind sie auf die Geschäftstätigkeit der ZADs zugeschnitten. Es wird das Geschäftsmodell überprüft,[74] es müssen interne Kontrollmechanismen vorhanden sein,[75] es müssen Verfahren aufgesetzt sein für den Umgang mit sensiblen Zahlungsdaten[76] und es müssen Sicherheitsprozesses bestehen für den Schutz der Zahlungsdienstnutzer.[77]

Weiter gehört zu den Bewilligungsvoraussetzungen, dass die Dritten Zahlungsdienstleister über eine Berufshaftpflichtversicherung verfügen müssen.[78] Damit wird vermieden, dass bei einer Risikoverwirklichung (betrügerische Belastungen des Kundenkontos, sonstiger Missbrauch von

---

71 Erw. 29 PSD2. Die finale Fassung der PSD2 enthält noch umfassendere Regelungen zum Daten- und zum Verbraucherschutz als der Kommissionsvorschlag, siehe dazu BÖGER, Neue Rechtsregeln, S. 263.

72 ZADs werden ausdrücklich als Zahlungsdienste erfasst: Anhang I Nr. 7 PSD2.

73 Art. 5, 11 Abs. 1 PSD2.

74 Art. 5 Abs. 1 lit. a PSD2.

75 Art. 5 Abs. 1 lit. e PSD2.

76 Art. 5 Abs. 1 lit. g PSD2.

77 Art. 5 Abs. 1 lit. j PSD2.

78 Art. 5 Abs. 2 PSD2 i.V.m. Anhang 1 Ziff. 7 und 8 PSD2. Siehe dazu auch Erw. 35 PSD2.

Kundendaten) die Anbieter ihre Zahlungsunfähigkeit anmelden und sich so aus der Verantwortung ziehen können.

b) Datenschutz

Die PSD2 enthält umfassende Regelungen hinsichtlich des Zugriffs und der Verwendung von Daten durch die Zahlungsauslösedienste und Kontoinformationsdienste. Sie müssen unter anderem sicherstellen, dass die personalisierten Sicherheitsmerkmale keiner andren Partei (ausser der Kundin und der kontoführenden Bank) zugänglich sind.[79] ZADs dürfen zudem keine sensiblen Zahlungsdaten der Kundin, namentlich ihre Bankzugangsdaten, speichern,[80] und sie dürfen nur die Daten verlangen, die für Zahlungsauslösedienstleistung notwendig sind.[81] ZADs und KIDs dürfen die erlangten Daten nicht zu anderen Zwecken als zu den ausdrücklich geforderten Dienstleistungen speichern oder verwenden.[82]

Die Datenschutzregelung ist also sehr restriktiv, denn damit wird die Verarbeitung dieser Daten zu kommerziellen Zwecken untersagt.[83] Für Kontoinformationsdienste dürfte dies aber den Kern des Geschäftsmodells bilden.

c) Identifikation des Zahlungsauslösedienstes

Zahlungsauslösedienste müssen sich gegenüber der Bank als solche identifizieren, wenn sie eine Zahlung in Auftrag geben.[84] Dies erlaubt es der Bank, den informationellen Zugriff des Zahlungsauslösedienstes auf das Konto zu beschränken, so dass nicht mehr die gesamte Zahlungshistorie eingesehen werden kann.

Ob dies über eine separate Schnittstelle erfolgt soll, oder – wie ursprünglich – ein Screen Scraping erlaubt sein soll, war lange Gegenstand von Diskussionen. Die EU-Kommission hat aber nun in ihren finalen technischen Regulierungsstandards (RTS) die Entscheidung zugunsten einer ausschliess-

79 Art. 66 Abs. 3 lit. c, Art. 67 Abs. 2 lit. b PSD2.
80 Art. 66 Abs. 3 lit. e PSD2.
81 Art. 66 Abs. 3 lit. f.
82 Art. 66 Abs. 3 lit. g, Art. 67 Abs. 2 lit. f PSD2.
83 BÖGER, Neue Rechtsregeln, S. 274.
84 Art. 66 Abs. 3 lit. d PSD2.

lichen Schnittstellenlösung getroffen. Nach Ablauf der Umsetzungsfrist (14. September 2019) wird das Screen Scraping nicht mehr erlaubt sein.[85]

d) Sicherheitspflichten

aa) Sichere Kommunikationskanäle

Sowohl die Dritten Zahlungsdienstleister als auch die Bank müssen sichere Kommunikationskanäle nutzen.[86] Die Kommission hat die Anforderungen in den RTS vom 27. November 2017 konkretisiert.[87]

bb) Qualifizierte starke Kundenauthentifizierung

Für eine erhöhte Sicherheit sorgt zudem die Pflicht, dass bei der Nutzung eines Zahlungsauslösedienstes eine starke Kundenauthetifizierung verlangt wird, die ein zusätzliches qualifizierendes Merkmal aufweist: Der Zahlungsvorgang wird dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpft.[88] Diese Pflicht ist aufsichtsrechtlicher Natur. Wie aber bereits dargelegt wurde, wirkt sie sich auch auf die Haftungslage aus.[89]

4. Technische Regulierungsstandards und Übergangsregelungen

In wesentlichen Punkten regelte die Richtlinie die Fragen der Dritten Zahlungdienstleister unter dem Vorbehalt dass die Einzelheiten noch durch technische Regulierungsstandards auszufüllen waren. Dies betraf insbesondere die Einzelheiten der starken Kundenauthetifizierung, die bei allen Fällen der Einschaltung von Zahlungsauslösediensten erfolgen muss.[90] Des Weiteren sollten auch die Einzelheiten der sicheren Kommunikation

---

85 Siehe Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23), Art. 30, 31. Zum Verbot des Screen Scraping siehe den ausdrücklichen Hinweis im Kommissionsentwurf C(2017) 7782 final S. 3.

86 Art. 66 Abs. 3 lit. b und d PSD2.

87 Delegierte Verordnung (EU) 2018/389 der Kommission [...].

88 Art. 97 Abs. 3 PSD2. Zur starken Kundenauthentifizierung eingehend SCHMID, (Starke) Kundenauthentifizierung, S. 76.; HOFFMANN, VuR 2016, S. 243 ff.

89 Art. 74 Abs. 2 PSD2: Das Fehlen einer starken Kundenauthentifizierung führt dazu, dass die Bank den Schaden für eine unautorisierte Zahlung auch dann selbst trägt, wenn die Kundin grob fahrlässig gehandelt hat.

90 Art. 97 Abs. 3 PSD2.

zwischen dem Zahlungsauslösedienst und der Bank noch durch technische Regulierungsstandards geregelt werden.[91]

Die EU-Kommission hat die RTS mittlerweile publiziert.[92] Sie gilt ab dem 14. September 2019. Für den Zugang zu den Kundenkonten über eine Schnittstelle gilt die Sonderfrist vom 14. März 2019.[93] Bis dahin gelten folgende Übergangsregelungen: Zahlungsauslösedienste, die bereits im Moment des Richtlinienerlasses tätig waren, geniessen Bestandesschutz und dürfen ihre Tätigkeit ohne besondere aufsichtsrechtliche Zulassung fortsetzen.[94] Ab dem Richtlinienerlass ist es den Banken untersagt, Zahlungsauslösedienste zu behindern oder zu blockieren.[95]

V. Schluss

Im Zahlungsverkehr hat die Digitalisierung zum Auftreten neuer Akteure auf dem Markt geführt. Unter diesen Akteuren sind solche, die für ihre Dienstleistung einen Zugang zum Bankkonto der Kundin benötigen. Das sind insbesondere die Kontoinformationsdienste und die Zahlungsauslösedienste. Das «Surfen auf der Bankinfrastruktur»[96] wirft Fragen im Hinblick auf den Wettbewerb, die Datensicherheit und den Datenschutz auf. Im Fokus des vorliegenden Beitrags standen die unautorisierten Transaktionen, die unter Nutzung eines Dritten Zahlungsdienstleisters erfolgten.

Dabei hat sich gezeigt, dass die Nutzung der neuen Angebote das Risiko von Phishing-Angriffen nicht exponentiell vergrössert. Würde es aber zu einem Angriff kommen, so wäre die Rechtslage in der Schweiz grundlegend anders als diejenige in der EU. In der Schweiz haben die Banken die Haftung für diese Fälle ausgeschlossen; die Nutzung eines Dritten Zahlungsdienstleisters unter Weitergabe der persönlichen Sicherheitsmerkmale ist eine Vertragsverletzung, die zur vollen Risikotragung der Kundin gegenüber der Bank führt. Anders verhält es sich in der EU. Diese hat mit der PSD2 den Markt für die Dritten Zahlungsdienste geöffnet und forciert in diesem Be-

91 Art. 98 Abs. 1 lit. d PSD2; Erw. 93 PSD2.

92 Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 (ABl Nr. L 69 v. 13.03.2018, S. 23).

93 Art. 38 RTS.

94 Art. 115 Abs. 5 PSD2.

95 Art. 115 Abs. 6 PSD2.

96 EMMENEGGER, Die Volkswirtschaft 6/2018, S. 48.

reich den Wettbewerb nicht zuletzt auch durch die primäre Haftung der Banken im Falle unautorisierter Transaktionen, mit Regressmöglichkeiten auf die Dritten Zahlungsdienstleister. Gleichzeitig verlangt aber die EU hohe Sicherheitsstandards und bindet die Dritten Zahlungsdienstleister in die Regulierung ein.

Das schafft für die Nutzerinnen und Nutzer von solchen Dienstleistungen mehr Sicherheit. Im dynamischen Markt der Dienstleistungen im Zahlungsverkehr wird sich in der Schweiz mittelfristig die Diskussion um die Regulierung von neuen Akteuren nicht vermeiden lassen. Spätestens dann ist die Diskussion um die Frage, ob die Bankkundin autonom entscheiden kann, wem sie den Zugriff zu seinem Konto gewährt, wieder auf dem Tisch.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 1. Mai 2018.

BAFIN JOURNAL, Zahlungsdiensterichtlinie II: Risiken und schwerwiegende Folgen für Nutzer und Kreditinstitute, verfasst von Josef Kokert und Markus Held, Juni 2014, S. 1–47.

BAUMBACH/HOPT HGB-BEARBEITER, Handelsgesetzbuch mit GmbH & Co., Handelsklauseln, Bank- und Kapitalmarktrecht, Transportrecht (ohne Seerecht), hrsg. von Klaus J. Hopt u.a., 38. Aufl., München 2018.

BÖGER OLE, Neue Rechtsregeln für den Zahlungsverkehr, in: Volker Gross u.a. (Hrsg.), Bankrechtstag 2016, Berlin 2017, S. 193–300.

DEUTSCHE KREDITWIRTSCHAFT, Stellungnahme der Deutschen Kreditwirtschaft zum Vorschlag der Europäischen Kommission zur Änderung der EU-Zahlungsdiensterichtlinie (PSD II), S. 1–15.

EMMENEGGER SUSAN, Die EU öffnet den Markt für neue Zahlungsdienstleister, Die Volkswirtschat 6/2018, S. 48–49.

EMMENEGGER SUSAN, PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 17–66.

GAUCH PETER/SCHLUEP WALTER R./SCHMID JÖRG/EMMENEGGER SUSAN, Schweizerisches Obligationenrecht, Allgemeiner Teil, Bd. I, 10. Aufl., Zürich 2014.

HOFFMANN JOCHEN, Kundenhaftung unter der Neufassung der Zahlungsdiensterichtlinie, VuR 2016, S. 243–254.

LINARDATOS DIMITRIOS, Der Kommissionsvorschlag für eine Zahlungsdiensterichtlinie II – Ein Überblick zu den haftungsrechtlichen Reformvorhaben, WM Heft 7/2014, S. 300–307.

OMLOR SEBASTIAN, Die zweite Zahlungsdiensterichtlinie: Revolution oder Evolution im Bankvertragsrecht?, ZIP 12/2016, S. 558–564.

SCHALLER JEAN MARC, Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Basel 2017, S. 45–70.

SCHMID FABIAN, (Starke) Kundenauthentifizierung: Aufsichtsrecht und Zivilrecht, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 67–85.

SCHOOR JULIUS S., «Sofortüberweisung». Sofort bezahlt. Sofort sicher?, S. 1–6.

SPINDLER GERALD/ZAHRTE KAI, Zum Entwurf für eine Überarbeitung der Zahlungsdiensterichtlinie (PSD II), BKR 2014, S. 265–271.

STENGEL CORNELIA, Unautorisierte Transaktionen in Zahlungssystemen: Am Beispiel von Twint, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 117–138.

TERLAU MATTHIAS, Die zweite Zahlungsdiensterichtlinie – zwischen technischer Innovation und Ausdehnung des Aufsichtsrechts, ZBB 2/2016, S. 122–137.

TERLAU MATTHIAS, SEPA Instant Payment – POS – und eCommerce-Abwicklung über Zahlungsauslösedienste und technische Dienstleister nach der Zweiten Zahlungsdiensterichtlinie (Payment Services Directive 2, PSD2), jurisPR-BKR 2/2016, Anm. 1, S. 1–18.

TRÜEB HANS RUDOLF/KEISER BARBARA A., Regulierung und Marktzutritt dritter Zahlungsdienstleister, S. 161–180.

Materialien

Hinweis: Zahlreiche der hier aufgeführten Dokumente sind über die gängigen Internetsuchmaschinen auffindbar. Auf die Angabe einer (häufig wechselnden) url wird daher verzichtet.

Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (ABl Nr. L 69 v. 13.03.2018, S. 23).

Delegierten Verordnung (EU) …/… der Kommission vom XXX zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, C(2017) 7782 final S. 1–34.

Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36 EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl Nr. L 337 v. 23.12.2015, S. 35).

Vorschlag (EU-Kommission) für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2013/36/EU und 2009/110/EG sowie zur Aufhebung der Richtlinie 2007/64/EG, COM(2013) 547 final vom 24.07.2013, S. 8.

Unautorisierte Transaktionen in Zahlungssystemen: Am Beispiel von Twint

Dr. Cornelia Stengel, Zürich*

Inhaltsverzeichnis

* Partnerin bei Kellerhals Carrard, Rechtsanwältin für Finanzdienstleistungsrecht und Datenschutz mit besonderer Erfahrung in der rechtlichen Analyse neuer Produkte, Systeme und Technologien auf dem Finanzmarkt (Fintech).
Die Autorin dankt TWINT AG für die zur Verfügung gestellte Dokumentation.

I. Fragestellung

TWINT ist ein *Zahlungssystem* oder in den Worten des FinfraG eine «Einrichtung, die gestützt auf einheitliche Regeln und Verfahren Zahlungsverpflichtungen abrechnet und abwickelt»[1]. TWINT ist ein *digitales* und *mobiles* Zahlungssystem, weil die Zahlungen auf digitalem, also elektronischem Weg und über mobile Geräte abgewickelt werden. Für diesen elektronischen Zahlungsverkehr wird elektronisches Geld (E-Geld) eingesetzt, die digitale Repräsentation einer offiziellen Währung. Kurz: TWINT ermöglicht bargeldloses Bezahlen an Kassen, Automaten, in Online- und App-Shops und zwischen Nutzern in der Schweiz.

Rund um Zahlungssysteme gibt es für Juristen viele interessante Fragestellungen. Vorliegend wird der zivilrechtliche Aspekt unautorisierter Transaktionen im TWINT-Zahlungssystem beleuchtet, also die Frage, wer den Schaden trägt, wenn über TWINT eine Transaktion von einem Konto ausgelöst wird, welche nicht vom Kontoinhaber autorisiert wurde.

Es sind beispielsweise folgende Konstellationen denkbar:

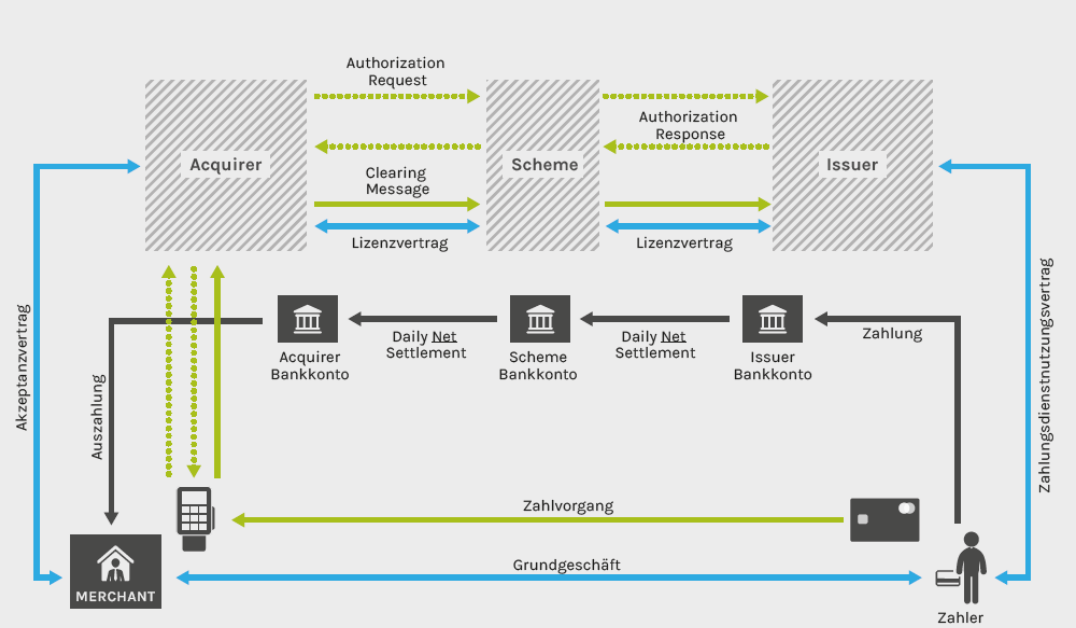
1) Ein TWINT-Nutzer sperrt sein Smartphone und seine TWINT-App mit einem Code, der seinem Jahrgang entspricht. Er (a) verliert das Telefon bzw. (b) das Telefon wird ihm gestohlen. Der Finder bzw. Dieb errät den Code und bezahlt über die TWINT-App verschiedene Einkäufe, welche in der Folge dem Bankkonto des TWINT-Nutzers belastet werden, mit welchem er die TWINT-App «verknüpft» hatte.
2) Ein TWINT-Nutzer hinterlegt in seiner TWINT-App eine fremde Kreditkarte bzw. verknüpft ein fremdes Bankkonto. Er bezahlt mit der TWINT-App, worauf das fremde Kartenkonto bzw. das fremde Bankkonto belastet wird.
3) Der Transaktionsbetrag für ein Grundgeschäft wird dem TWINT-Nutzer mehrfach belastet.

Um die eingangs gestellte Frage nach der Schadenstragung zu beantworten, müssen vorab die grundlegenden Begriffe definiert und das Modell des TWINT-Zahlungssystems mit den daran beteiligten Parteien, dem Ablauf einer Transaktion und den vertraglichen Beziehungen zwischen den Parteien geklärt werden.

[1] Art. 81 FinfraG.

II. Grundlagen: Vier- bzw. Mehrparteiensystem[2]

1. Schema



Modell und Grafik: Cornelia Stengel/Thomas Weber, Digitale und mobile Zahlungssysteme, Schulthess 2016.

2. Beschreibung

Das Vier- bzw. Mehrparteiensystem kann als «Mutter» der digitalen Zahlungssysteme bezeichnet werden, da die allermeisten existierenden, digitalen Zahlungssysteme in dieser Art aufgebaut sind.

Als Beispiele sind die in der Schweiz bekanntesten und relevantesten, sogenannten «Kreditkartensysteme»[3] von MasterCard und Visa zu nennen.

In der Branche (und auch in den einschlägigen Verordnungen der EU)[4] wird das Mehrparteiensystem – insb. mit Blick auf das Dreiparteiensystem[5]

---

2 Die Ausführungen zu den Grundlagen basieren auf dem Buch: STENGEL CORNELIA/WEBER THOMAS, Digitale und mobile Zahlungssysteme.

3 Dem Begriff «Kreditkarte» kommt in unterschiedlichen Zusammenhängen unterschiedliche Bedeutung zu (z.B. als Hinweis auf eine Abrechnungsart mit Kreditfunktion; vgl. dazu STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 15 u. 142), weshalb nachfolgend stattdessen von «Zahlkarten» und entsprechend von «Zahlkartensystemen» gesprochen wird.

4 EU VO IFR Art. 2 (17) – Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge.

und als Abgrenzung zu verschiedenen anderen Mehrparteiensystemen (Wallets)[6] – regelmässig als «Vierparteiensystem» bezeichnet. Gemeint ist aber ein- und dasselbe System, an welchem (mindestens)[7] fünf Parteien beteiligt sind, nämlich der Zahler, der Merchant oder Händler, ein Issuer und ein Acquirer sowie das Scheme.

3. Beteiligte Parteien

Der *Zahler*[8] ist jene Person, die einen Zahlungsauftrag erteilt. Das wäre beispielsweise der Kunde oder die Kundin, der bzw. die für ein Buch bezahlen möchte, welches er oder sie soeben gekauft hat.

Der Begriff *Merchant*[9] (auch *Händler* oder *Akzeptanzstelle*) meint jene natürliche oder juristische Person, welche die Zahlung über das digitale Zahlungssystem erhalten soll, also den Zahlungsempfänger. In unserem Beispiel wäre das der Buchhändler.

Der *Issuer*[10] stellt dem Zahler ein Zahlungsinstrument zur Verfügung, beispielsweise eine Zahlkarte oder – vorliegend relevant – eine entsprechende App, mit welcher der Zahler eine digitale Zahlung veranlassen kann. Im Falle eines Zahlkartensystems wird der Issuer auch *Zahlkartenherausgeber* oder kurz: *Herausgeber* genannt. In der Schweiz sind beispielsweise Swisscard, Viseca Card Services, UBS Card Center und Cornèr Card als Issuer bekannt.

---

5 Am Dreiparteiensystem ist nebst dem Zahler und dem Merchant nur noch das Scheme beteiligt, welches gleichzeitig auch die Rollen von Issuer und Acquirer übernimmt. Beispiele: Postcard, American Express; vgl. STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 149 ff.

6 Vgl. beispielsweise Staged Wallet (STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 174 ff.); Top-up Wallet (STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 190 ff.); Pass-through Wallet (STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 204 ff.).

7 In der vorliegenden Beschreibung wird das Scheme als Kombination von Lizenzgeber und (technisches) Zahlungsnetzwerk definiert.

8 Vgl. auch die Definition nach EU RL PSD II Art. 4 (8) – Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge.

9 Vgl. auch die Definition nach EU RL PSD II Art. 4 (9).

10 Vgl. auch die Definition für *Emittent* nach EU VO IFR Art. 2 (2).

Damit der Merchant, unser Buchhändler, die Zahlung seines Kunden via ein digitales Zahlungssystem entgegennehmen kann, schliesst er einen Vertrag mit einem *Acquirer*[11] ab. Der Acquirer bindet den Merchant technisch und prozessual an das entsprechende Zahlungssystem an und wickelt seine Transaktionen und Geldflüsse ab. Der grösste Acquirer der Schweiz ist SIX.

Das *Scheme* betreibt das digitale Zahlungssystem und nimmt dabei regelmässig sowohl die Rolle des Lizenzgebers als auch jene des (technischen) Zahlungsnetzwerks ein. Es lizenziert die Issuer und Acquirer zur Nutzung seiner operativen und technischen Spezifikationen, seiner Marke und der gesamten Infrastruktur des Zahlungssystems. Dabei erlässt es detaillierte Regeln, sog. *Scheme Rules*, betreffend die Tätigkeiten der Lizenznehmer, die technischen Schnittstellen, Prozesse, Transaktionen etc. Gleichzeitig stellt das Scheme als zentrale Abwicklungsstelle die technische Abwicklung der Transaktionen und Geldflüsse sicher.[12] Das Scheme gibt dem Zahlungssystem meist auch den Namen, wie beispielsweise MasterCard, VISA oder eben TWINT.

4. Ablauf einer digitalen Zahlung

Der Ablauf einer digitalen Zahlung lässt sich in die folgenden fünf Teile gliedern, welche nachfolgend kurz zusammenfassend[13] erläutert werden:

- Einsatz des Zahlungsinstruments
- Authentisierung und Authentifikation des Zahlers
- Autorisation zwischen Issuer und Acquirer
- Clearing
- Settlement

Basierend auf dem Grundgeschäft zwischen Zahler und Merchant (z. B. der Kauf eines Buches) nutzt der Zahler sein Zahlungsinstrument zur Bezahlung des Merchants. Beim *Zahlungsinstrument*[14] handelt es sich um jenes persona-

11 Vgl. auch die Definition nach EU VO IFR Art. 2 (1).

12 Aufgrund regulatorischer Vorgaben in der EU müssen diese beiden Rollen zukünftig getrennt werden (vgl. EU VO IFR Art. 7).

13 Für eine detaillierte Beschreibung vgl. STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 54 ff., Grafik: N 117.

14 EU RL PSD II Art. 4 (14); teilweise wird das Zahlungsinstrument in der Schweizer Geldwäschereigesetzgebung als *Zahlungsmittel* bezeichnet, wobei letzterer Begriff nicht konsistent verwendet wird (vgl. STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 20 ff.).

lisierte Instrument, welches gemäss der Vereinbarung zwischen Issuer und Zahler zur Erteilung eines Zahlungsauftrags an den Issuer dient, beispielsweise den EMV-Chip[15] auf einer Zahlkarte oder der App[16] bei TWINT. Dabei werden die Daten des Zahlungsinstruments an den Merchant bzw. sein Terminal oder seine Applikation übermittelt. Für diesen Vorgang stehen verschiedene technologische Varianten zur Verfügung, je nachdem ob es sich um eine Transaktion bei einer physischen Verkaufsstelle oder einer im Internet (Online-Store) handelt. Beispiele sind das Auslesen der Magnetspur oder des EMV-Chips einer Zahlkarte, wobei dies auch kontaktlos, z.B. über eine NFC-Schnittstelle[17] geschehen kann.

Im Falle von TWINT erfolgt diese Übertragung mittels *Bluetooth*[18] über einen sogenannten Beacon oder mittels Scannen eines *QR-Codes*[19]. Entweder

15 Der EMV-Chip wurde von Europay, MasterCard und Visa im Jahr 1993 lanciert und löste die Magnetspurtechnologie ab. Heute wird der EMV-Standard (ISO/IEC 7816, 14444) von allen massgeblichen Schemes über die Organisation EMVCo verwaltet und weiterentwickelt. EMVCo ist inzwischen auch für die Spezifikationen von Tokenisierungen und 3-D Secure verantwortlich.

16 Bzw. die Payment Section der TWINT-Applikation.

17 Near Field Communication (NFC) ist ein Funkprotokoll zur Abwicklung von Mobile Payment-Zahlungen in physischen Verkaufsstellen. Im Vergleich zur Bluetooth-Technologie verbraucht NFC weniger Energie und durch die von der NFC-Technologie erforderliche Nähe werden Signalstörungen durch andere Geräte minimiert. Auch erfolgt eine NFC-Kopplung zwischen mehreren Geräten fast sofort und bedarf keiner manuellen Verbindung wie eine Bluetooth-Kopplung. Schliesslich verfügen viele der derzeit bei Händlern eingesetzten Zahlungsterminals über eine NFC-Schnittstelle, zumal kontaktlose Zahlungen mit physischen Debit- und Kreditkarten ebenfalls auf NFC basieren. Bezüglich der Nutzung von NFC im Bereich Mobile Payment besteht die Einschränkung, dass Apple Drittanbietern von Mobile Payment-Apps keinen Zugriff auf die NFC-Schnittstelle bei iPhones gewährt (RPW 2016/4 S. 1062 ff., 26).

18 Diese Funktechnologie hat den Vorteil, dass sie praktisch auf allen Smartphones (unabhängig vom Betriebssystem) vorhanden und Entwicklern von Apps zugänglich ist. Allerdings verfügen die üblichen durch Merchants eingesetzten Terminals meist nicht über eine Bluetooth-Funktionalität, so dass im Falle von TWINT zusätzlich sogenannte Beacons zum Einsatz kommen (RPW 2016/4 S. 1062 ff., 25).

19 Alternativ kann auch ein Zahlencode zum Einsatz kommen, welcher (beispielsweise auf der Website eines Online-Stores) angezeigt wird und manuell in der Zahlungs-App eingegeben wird. Wie auch Bluetooth haben QR-Codes sowie Zahlencodes den Vorteil, dass diese bei sämtlichen modernen Smartphones eingesetzt werden können und die entsprechenden Schnittstellen Entwicklern bei sämtlichen mobilen Betriebssystemen offenstehen (RPW 2016/4 S. 1062 ff., 27).

erhält also die TWINT-App des Zahlers mittels Bluetooth-Signal vom Terminal des Merchants die Daten, um den Merchant und den Transaktionsbetrag zu bestimmen, oder dieser Datentransfer wird über das Abscannen eines vom Merchant generierten QR-Codes abgewickelt.

Auch die Art der *Authentisierung*[20] *und Authentifikation*[21] *des Zahlers* hängt von den technischen Möglichkeiten der eingesetzten Infrastruktur des Merchants und des Zahlungsinstruments sowie dem Risikogehalt der Transaktion ab. Zur Authentifikation können beispielsweise ein Kartenablaufdatum, der CVC2 bzw. CVV2[22], die Unterschrift des Zahlers, eine PIN oder 3-D Secure-Verfahren dienen oder sie erfolgt biometrisch (Fingerabdruck, Gesicht). Aufgrund bewusster Risikoentscheide können die Issuer aber auch auf eine Authentifikation des Zahlers verzichten. Dies ist in der Schweiz beispielsweise bei kontaktlosen Bezahlungen bis CHF 40 üblich. Bei TWINT wird der Zahler durch Eingabe einer PIN authentifiziert.

Nach erfolgter Authentifikation des Zahlers muss die Zahlung durch den Issuer autorisiert werden (*Autorisation zwischen Issuer und Acquirer*).[23] Das Terminal bzw. die Applikation des Merchants sendet eine Autorisationsanfrage (*Authorization Request*) an den Acquirer, welcher sie an das Scheme weiterleitet. Das Scheme wiederum leitet die Anfrage an den Issuer weiter, welcher die Anfrage prüft und eine Entscheidung fällt (*Authorization Decision*). Die Entscheidung wird als Antwort (*Authorization Response*) über das Scheme an den Acquirer zurückgeleitet, der wiederum das Terminal bzw. die Applikation des Merchants entsprechend informiert. Eine erfolgreiche Autorisation erkennen Merchant und Zahler jeweils an einem entsprechenden Zeichen (z.B. grünes Häklein, Ton).

Nach der Autorisation reicht der Merchant über sein Terminal bzw. seine Applikation die Transaktion an den Acquirer ein, welcher den Betrag dem Merchantkonto gutschreibt und das *Clearing* im Batch-Verfahren an das Scheme leitet. Dieses wiederum stellt die Weiterleitung an den Issuer sicher, welcher schliesslich das Zahlungskonto des Zahlers belastet.

---

20 Der Nutzer erbringt einen Nachweis seiner Identität.

21 Prüfung des Nachweises der Identität, welchen der Nutzer erbracht hat, also Prüfung der Authentisierung (i.d.R. durch den Issuer).

22 Card Validation Code 2 (Begriff MasterCard) bzw. Card Validation Value 2 (Begriff Visa).

23 Diese Autorisation ist von der Autorisation zwischen Zahler und Issuer zu unterscheiden, mit welcher der Zahler den Issuer zur Belastung seines Zahlkontos ermächtigt.

Das Scheme vergütet den Acquirer, wobei die im Scheme vereinbarten Gebühren für das Scheme und den Issuer abgezogen werden, und belastet den Issuer (*Settlement*). Im klassischen Vierparteiensystem geschieht dies basierend auf dem *Daily-Net-Settlement-Prinzip*[24].

Je nach Funktion des Zahlkontos des Zahlers bzw. der mit dem Issuer vereinbarten *Abrechnungsart*[25] begleicht der Zahler die Forderung des Issuers für die belasteten Transaktionen. Der Acquirer bezahlt dem Merchant die eingereichten und auf dem Merchantkonto verbuchten Transaktionen, abzüglich Gebühren, auf dessen Bankkonto aus.

5. Vertragliche Beziehungen

a) Mehrgliedrige Anweisung

Die einzelnen Verträge in einem Vier- bzw. Mehrparteien-Zahlungssystem können nicht unabhängig voneinander betrachtet werden. Sie sind teilweise explizit, teilweise implizit und systembedingt miteinander verbunden. Dazu kommt, dass die Parteien entweder vertraglich oder faktisch an die Regeln des jeweiligen Zahlungssystems, die sogenannten Scheme Rules, gebunden sind, was wiederum starken Einfluss auf die Beziehungen und Verträge zwischen den Parteien hat.

Die vertragsrechtliche Grundlage solcher Zahlungssysteme ist eine mehrgliedrige Anweisung im Sinne von Art. 466 ff. OR[26], an deren Anfang

---

24 Das Settlement findet einmal am Tag zwischen Issuer und Scheme sowie zwischen Scheme und Acquirer statt. Das Scheme berechnet auf Basis aller in das Clearing eingelieferten Transaktionen die Interchange Fee sowie die Scheme-Gebühren. Der Acquirer erhält somit die Summe aller Transaktionsbeträge abzüglich der errechneten Totalsumme Interchange Fee und Scheme-Gebühren in der vereinbarten Währung ausbezahlt. Die Auszahlung wird mittels Banküberweisung vom Bankkonto des Schemes auf das Bankkonto des Acquirers getätigt. Das Scheme informiert den Issuer täglich über den fälligen Betrag. Dieser setzt sich aus der Summe aller zu Lasten des Issuers in das Clearing eingelieferten Transaktionen, abzüglich der totalen Summe der Interchange Fees, zuzüglich der Scheme-Gebühren zusammen. Der Issuer überweist die fällige Summe von seinem Bankkonto auf das Bankkonto des Schemes.

25 Credit (Kredit- oder Teilzahlungsoption), Charge (Deferred Debit) oder PrePaid, Debit (vgl. STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 30 ff.).

26 STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 171 ff.; grundsätzlich ähnlich: ARTER, Kreditkartenzahlung, S. 284; GIGER, Kreditkartensystem, S. 191 f.; WÜRSCH, Kreditkarte nach schweizerischem Privatrecht, S. 171 f.; für das deutsche Recht: LANGENBUCHER, Risikozuordnung, S. 243 ff.; für Banküberweisungen: BGE 132 III 609,

die Anweisung des Zahlers an seinen Issuer steht. Mittels Übergabe der Daten seines Zahlungsinstruments an den Merchant und (falls erforderlich) einer Authentifikation durch PIN-Eingabe o.ä., weist der Zahler den Issuer an, dem Merchant (indirekt über das Scheme und den Acquirer) den entsprechenden Betrag zu vergüten. Damit *autorisiert* der Zahler gegenüber dem Issuer die Transaktion über das Zahlungssystem bzw. die Bezahlung des Merchants. Der Vertrag zwischen Issuer und Zahler bildet dabei das Deckungsverhältnis und der Vertrag zwischen Zahler und Merchant das Valutaverhältnis.[27]

Die Anweisung in einem Zahlungssystem weicht in einigen Punkten von der gesetzlichen Form ab. So erfolgt sie *indirekt* mittels Autorisierung über den jeweiligen Merchant (sowie über dessen Acquirer und das Scheme) und wird nicht direkt gegenüber dem Issuer erteilt. Der Issuer als Angewiesener verpflichtet sich unter gewissen *Bedingungen* (insb. korrekte Autorisierung der Zahlung, Einhaltung Ausgabelimite etc.) bereits *im Voraus* zur Ausführung der Anweisung bzw. Zahlung. Die Ausführung der Anweisung erfolgt wiederum nicht direkt durch Annahmeerklärung und Zahlung des Issuers an den Merchant, sondern *indirekt* über Scheme und Acquirer. Die in Zahlungssystemen regelmässig *fehlende Annahmeerklärung* des Issuers gegenüber dem Merchant wird durch ein (abstraktes, bedingtes) Schuldversprechen des Acquirers im Sinne von Art. 13 OR ersetzt, welches in den Scheme-Rules zwingend vorgesehen ist. Und schliesslich ist in einem Zahlungssystem die Anweisungserklärung des Zahlers systembedingt *unwiderruflich*.[28]

b) Die einzelnen Verträge zwischen den Parteien

So viele verschiedene digitale Zahlungssysteme existieren, so viele verschiedene Arten des Vertrags zwischen einem Zahler und seinem Issuer (*Zahlungsdienstnutzungsvertrag*) gibt es. Sie unterscheiden sich insbesondere auf-

---

S. 616, E. 5.1; BGE 127 III 553, S. 556, E. 2. c); BGE 126 III 20, S. 21 f., E. 3 a) aa) m.w.H.; BGE 121 III 109, S. 111 f., E. 2.

27 WÜRSCH 1975 S. 173 f.; KELLER, Kreditkarten, S. 169 f.; GIGER, Kreditkartensystem, S. 191 f.; GOETZ, Das internationale Kreditkartenverfahren, S. 29 f.; ARTER/JÖRG, Rückbelastungsklauseln, S. 26 f. m.H.a. CUSTODIS, Kreditkartenverfahren, S. 42 ff. und KIENHOLZ Die Zahlung mit Kreditkarten, S. 111; STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 260 ff.

28 Ausführlich und m.w.H. STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 272 f.

grund der verschiedenen Dienstleistungen, welche die verschiedenen Issuer anbieten, aber auch hinsichtlich der Haftungsregelungen, welche für die Beantwortung der eingangs gestellten Frage relevant sind. Allen Zahlungsdienstnutzungsverträgen ist jedoch gemeinsam, dass die Hauptpflicht des Issuers darin besteht, dem Zahler den bargeldlosen Bezug von Waren und Dienstleistungen zu ermöglichen, während die Hauptpflicht des Zahlers in der Begleichung des Abrechnungssaldos über die getätigten Transaktionen besteht.[29]

Auch zwischen dem Merchant und seinem Acquirer wird ein Vertrag abgeschlossen (*Akzeptanzvertrag*). Dieser ermöglicht dem Merchant die Anbindung an das digitale Zahlungssystem und damit den Zugang zum bargeldlosen Zahlungsverkehr über dasselbe. Der Merchant wird befähigt, eine bargeldlose Zahlung von seinem Kunden, dem Zahler, entgegen zu nehmen. Der Acquirer übernimmt entsprechend hauptsächlich das Clearing dieser Zahlungen und eine (bedingte) Zahlungsgarantie bzw. Übernahme des Debitorenrisikos, kann aber auch diverse Zusatzleistungen wie beispielsweise die Lieferung statistischer Informationen erbringen. Im Gegenzug verpflichtet sich der Merchant hauptsächlich zur Bezahlung einer Kommission.[30]

Das *Grundgeschäft* zwischen Zahler und Merchant ist unabhängig davon, ob bargeldlos über ein digitales Zahlungssystem bezahlt wird. Oder anders herum: Durch den Einsatz eines Zahlungsinstruments anstelle einer Barzahlung wird das Grundgeschäft in seiner rechtlichen Natur nicht berührt. Es kann sich dabei je nach Einzelfall beispielsweise um einen Kauf- oder Werkvertrag oder um einen Auftrag handeln. Die einzige Besonderheit in Zusammenhang mit dem Grundgeschäft besteht in der Abrede zwischen Zahler und Merchant, dass ersterer seine Geldleistungspflicht nicht in bar, sondern mittels Einsatz eines digitalen Zahlungsinstruments erfüllt (*Zahlungsformabrede*).

Damit ein Vier- oder Mehrparteien-Zahlungssystem funktioniert, braucht es schliesslich auch das Scheme, welches jeden Issuer und jeden Acquirer mittels *(Lizenz-)Vertrag* in das System einbindet. Damit erhalten

---

29 Vgl. zum Zahlungsdienstnutzungsvertrag, seiner rechtlichen Qualifikation und Abrechnungsarten bzw. Zinserhebungsmechanismen: STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 275 ff. mit diversen Hinweisen auf weiterführende Literatur, AGB-Klauseln und Gerichtsentscheide.

30 Vgl. weiterführend zum Akzeptanzvertrag: STENGEL/WEBER, Digitale und mobile Zahlungssysteme, N 338 ff. mit diversen Hinweisen auf weiterführende Literatur, AGB-Klauseln und Praxis.

diese hauptsächlich das Recht, am System teilzunehmen und die Marke des Schemes zu nutzen. Gleichzeitig verpflichten sie sich zur Einhaltung der Regeln des jeweiligen Zahlungssystems (*Scheme Rules*) und zur Bezahlung der Scheme-Gebühren. Die Scheme Rules sind standardisierte Regelwerke, also eine Art allgemeine Geschäftsbedingungen, welche bei der Nutzung des entsprechenden Zahlungssystems für die involvierten Acquirer, Issuer und das Scheme selbst gelten, aber auch Auswirkungen auf die eingebundenen Merchants und Zahler haben. Die Scheme Rules werden in der Regel vom Scheme einseitig erlassen und enthalten u.a. generelle Pflichten der beteiligten Parteien, Regeln für die Durchführung der Transaktionen, Haftungsregeln, Sicherheitsregeln und Gebührenstruktur.

Die Scheme Rules von TWINT entsprechen weitgehend jenen von MasterCard und Visa, welche öffentlich einsehbar sind.[31]

6. Das TWINT-Zahlungssystem

TWINT ist ein solches, oben beschriebenes Vier- bzw. Mehrparteiensystem und funktioniert damit im Wesentlichen gleich wie die Kartensysteme von VISA und MasterCard, wobei das Zahlungsinstrument nicht auf einer Zahlkarte, sondern in der TWINT-App enthalten ist.

Im TWINT-Zahlungssystem handelt die TWINT AG als Scheme. TWINT-Acquirer und damit Vertragspartner für die Merchants, welche TWINT-Zahlungen akzeptieren wollen, sind derzeit die SIX Payment Services und die TWINT Acquiring AG. Auf der anderen Seite können die Zahler aus den folgenden Unternehmen ihren TWINT-Issuer auswählen: TWINT AG, UBS, Zürcher Kantonalbank, PostFinance, Raiffeisen, Credit Suisse, Banque Cantonal Vaudoise, Obwaldner Kantonalbank, Zuger Kantonalbank, Banque Cantonal de Genève und Neue Aargauer Bank. Alle diese Unternehmen haben eine eigene TWINT-App entwickelt und schliessen mit den Zahlern eigene (und durchaus unterschiedliche) Verträge, sogenannte *Zahlungsdienstnutzungsverträge*, auch als *Nutzungsbedingungen* oder *Allgemeine Geschäftsbedingungen* bezeichnet, ab.

Die Einbindung eines Bankkontos (oder einer Kreditkarte) in der TWINT-App wird nur für das Auffüllen (*Funding*) der App bzw. den Ausgleich des Abrechnungssaldos des Issuers durch den Zahler und nicht direkt

[31] Vgl.: <https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf> und <https://www.visaeurope.com/about-us/policy-and-regulation/veor>.

für die Zahlung selbst verwendet. Bei einer Bezahlung via TWINT handelt es sich deshalb immer um eine Transaktion des TWINT-Schemes.[32] Daraus ergibt sich, dass (im Gegensatz zu einer Wallet-Lösung[33]) die Akzeptanz von TWINT durch einen Merchant eine explizite vertragliche Vereinbarung mit einem TWINT-Acquirer bedingt. Auf der anderen Seite schliessen die Zahler im TWINT-System einen Vertrag mit einem der verschiedenen TWINT-Issuer und laden dessen TWINT-App auf ihr Smartphone herunter.

Jeder TWINT-Issuer hat seine eigene TWINT-Applikation (*TWINT-App*) mit eigenen Funktionalitäten und – für den vorliegenden Beitrag relevant – auch mit einem eigenen Zahlungsdienstnutzungsvertrag entwickelt.

Praktisch läuft das in der Regel so ab, dass der TWINT-Nutzer die TWINT-App seiner Hausbank auf sein Smartphone herunterlädt und im Zuge der Installation derselben den entsprechenden Vertrag akzeptiert. Gehört die Hausbank des Nutzers nicht zu den TWINT-Issuern, so wird ihm vorgeschlagen die TWINT-App von TWINT AG zu verwenden.[34]

Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass TWINT neben diesen Peer-to-Merchant- bzw. *P2M-Zahlungen*[35] auch Peer-to-Peer- bzw. *P2P-Zahlungen*[36] ermöglicht.

---

32 RPW 2016/4 S. 1062 ff., 23.

33 Zu diesem Unterschied vgl. auch den Blog-Beitrag der Autorin vom 20. Februar 2018: «Zahlungssystem ist nicht gleich Zahlungssystem», abrufbar unter: <https://www.blog.paymentsystems.ch/2017/02/20/zahlungssystem-ist-nicht-gleich-zahlungssystem/>.

34 Vgl. Webseite von TWINT: <https://www.twint.ch/bank/twint/> (letzter Besuch: 13.01.2018). Damit wird die Verwirrung der Nutzer der verschiedenen TWINT-Apps reduziert.

35 Zahlungen von Privatpersonen an Merchants bzw. Händler (RPW 2016/4 S. 1062 ff., Fn 6); TWINT bezeichnet diese Funktion als «*Zahlen*».

36 Zahlungen zwischen Privatpersonen, meist kleinerer Beträge, von Mobile zu Mobile; P2P-Zahlungen funktionieren als Bargeld-Ersatz und eignen sich für kleinere Beträge und Transaktionen. Die Teilnehmer müssen nur die Mobile-Nummer des jeweiligen Partners kennen, um Geld anzufordern oder Geld zu überweisen (vgl. RPW 2016/4 S. 1062 ff., Fn 5); ähnlich: <https://www.iso-20022.ch/lexikon/p2p-payment/>; TWINT bezeichnet diese Funktion als «*Senden*».

III. Schadenverteilung bei unautorisierten Transaktionen

1. Die drei zu prüfenden Regelungsebenen

Der vorliegende Beitrag soll die eingangs gestellte, zivilrechtliche Frage klären, wer den Schaden im Falle nicht autorisierter Transaktionen trägt, wenn also über TWINT eine Transaktion von einem Konto ausgelöst wird, welche nicht vom Kontoinhaber autorisiert wurde. Geprüft werden die folgenden, ausgewählten Konstellationen 1–3:

1) Ein TWINT-Nutzer sperrt sein Smartphone und seine TWINT-App mit einem Code, der seinem Jahrgang entspricht. Er (a) verliert das Telefon bzw. (b) das Telefon wird ihm gestohlen. Der Finder bzw. Dieb errät den Code und bezahlt über die TWINT-App verschiedene Einkäufe, welche in der Folge dem Bankkonto des TWINT-Nutzers belastet werden, mit welchem er die TWINT-App «verknüpft» hatte.
2) Ein TWINT-Nutzer hinterlegt in seiner TWINT-App eine fremde Kreditkarte bzw. verknüpft ein fremdes Bankkonto. Er bezahlt mit der TWINT-App, worauf das fremde Kartenkonto bzw. das fremde Bankkonto belastet wird.
3) Der Transaktionsbetrag für ein Grundgeschäft wird dem TWINT-Nutzer mehrfach belastet.

Neben einer allfälligen (Diebstahl-) Versicherung des Zahlers, welche hier im Folgenden ausser Acht gelassen wird, kommen für die Schadenübernahme grundsätzlich alle Parteien des TWINT-Zahlungssystems in Frage, also der Zahler selbst, sein Issuer, der Merchant, dessen Acquirer oder das Scheme.

Wie oben beschrieben, sind die Beziehungen zwischen diesen Parteien durch verschiedene Verträge geregelt. Daneben sind ggf. auch gesetzliche bzw. regulatorische Vorgaben zu beachten. Daraus ergeben sich für TWINT – wie für jedes klassische Vier- bzw. Mehrparteien-Zahlungssystem – drei Prüfungsebenen. Zu prüfen ist aus Sicht des Zahlers vorab die vertragliche Vereinbarung zwischen dem Zahler und seinem Issuer, vorliegend also der TWINT-Zahlungsdienstnutzungsvertrag. Die zweite Ebene bilden die Scheme Rules, welche ebenfalls Regeln zur Schadenverteilung enthalten. Und schliesslich können in einer dritten Ebene gesetzliche bzw. regulatorische Vorgaben zu einer Veränderung der (vertraglichen) Schadentragung führen.

2. Zahlungsdienstnutzungsverträge

a) Verschiedene Bestimmungen zur Schadenübernahme

Will unser Beispiel-Kunde herausfinden, ob er den Betrag, welcher mit seiner TWINT-App ausgegeben wurde, selbst bezahlen muss oder ob jemand diesen Schaden übernimmt, schaut er zuerst in den Vertrag mit seinem TWINT-Issuer, also den Zahlungsdienstnutzungsvertrag bzw. die entsprechenden Nutzungsbedingungen, welche er im Zuge der Installation der TWINT-App akzeptiert hat.

Wie oben beschrieben, gibt es nicht eine einzige TWINT-App mit Nutzungsbedingungen. Vielmehr hat jeder TWINT-Issuer seine eigene TWINT-App mit eigener Funktionalität entwickelt und eigene Nutzungsbedingungen «erlassen». Zwar gleichen sich diese Nutzungsbedingungen, weil die Scheme Rules viele Faktoren vorgeben. Gerade bei der Schadenübernahme gibt es aber Unterschiede. Es kommt für den Kunden also schon darauf an, mit welchem TWINT-Issuer er einen Vertrag abschliesst bzw. welche TWINT-App er auf sein Smartphone herunterlädt.

Im Folgenden werden die Nutzungsbedingungen von drei TWINT-Issuern mit Blick auf die eingangs gestellte Frage genauer geprüft:

Die Schadenübernahme von **TWINT AG** ist in den Ziff. 1.8 und 1.9 der AGB von TWINT AG geregelt. Danach übernimmt TWINT AG Schäden, die dem Kunden aus missbräuchlicher Verwendung der TWINT-App durch Dritte entstehen, sofern er (der Kunde) nachzuweisen vermag, dass er die AGB eingehalten hat und ihn auch sonst in keiner Weise ein Verschulden trifft. Pro Schadenereignis werden allerdings höchstens CHF 5'000 für direkte Schäden übernommen, wobei auch diese Schadenübernahme bei bloss leichter Fahrlässigkeit seitens des Kunden von TWINT AG wieder ausgeschlossen wird.[37]

Die Sorgfaltspflichten eines Kunden von TWINT AG finden sich in Ziff. 1.6 der entsprechenden AGB. Demgemäss hat der Kunde *insbesondere* folgende Sorgfaltspflichten zu beachten:[38]

- Der Kunde hat sein Smartphone vor unbefugter Benutzung oder Manipulation zu schützen (z.B. mittels Geräte- bzw. Displaysperre).

[37] Version abgerufen am 16.12.2017.

[38] Wörtliches Zitat, Version abgerufen am 16.12.2017.

- Der Code für die Nutzung der TWINT App, insbesondere für Ladungen/Entladungen sowie zur Bestätigung von Zahlungen ab einem bestimmten Betrag, sowie die Codes der Geräte- bzw. Displaysperren, sind geheim zu halten, dürfen keinesfalls an andere Personen weitergegeben, oder zusammen mit dem Smartphone aufbewahrt werden.
- Der gewählte Code darf nicht aus leicht ermittelbaren Kombinationen (Mobile-Nummer, Geburtsdatum usw.) bestehen.
- Im Schadenfall hat der Kunde nach bestem Wissen zur Aufklärung des Falls und zur Schadensminderung beizutragen. Bei strafbaren Handlungen hat er Anzeige bei der Polizei zu erstatten.
- Mit der Installation der TWINT App auf seinem Smartphone bestätigt der Kunde, der rechtmässige Nutzer und Verfügungsberechtigte der Mobile-Nummer des Smartphones zu sein. Der Kunde ist für die Verwendung (Nutzung) seines Smartphones verantwortlich. Der Kunde trägt sämtliche Folgen, die sich aus der Verwendung der TWINT App auf seinem Smartphone ergeben.
- Besteht Grund zur Annahme, dass unberechtigte Personen Zugang zur Geräte- bzw. Displaysperre haben, so ist diese unverzüglich zu ändern.
- Bei Verlust des Smartphones, insbesondere im Falle eines Diebstahls, ist die TWINT AG umgehend zu benachrichtigen, damit eine Sperrung der TWINT App erfolgen kann.

Die Nutzungsbedingungen der **Raiffeisen** TWINT-App sehen keine Maximalgrenze für die Schadenübernahme vor. Im Übrigen sind die Haftungsregeln im Resultat mit jenen von TWINT AG identisch. Gemäss Ziff. 14 übernimmt Raiffeisen direkte Schäden, die dem Kunden aus der missbräuchlichen Verwendung der Raiffeisen TWINT-App durch Dritte entstehen, wenn der Kunde die Bedingungen für die Benützung der Raiffeisen TWINT-App eingehalten hat und ihn auch sonst in keiner Weise ein Verschulden trifft. Auch die Sorgfaltspflichten des Nutzers, welche sich bei Raiffeisen TWINT aus Ziff. 8 der AGB ergeben, sind mit jenen von TWINT AG vergleichbar.[39]

Dasselbe gilt bei einer Verwendung der TWINT-App von **Credit Suisse**, auch wenn die einschlägige Ziff. 1.6 «umgekehrt» formuliert festhält, dass eine Entschädigung des Kunden für Schäden, die dem Kunden wegen missbräuchlicher Nutzung der Credit Suisse TWINT-App entstehen, grundsätzlich ausgeschlossen sei, ausser, wenn der Kunde nachzuweisen vermag, dass ihm trotz Einhaltung seiner Pflichten gemäss diesen Nutzungsbedingungen

[39] Version 1.0 – Mai 2017, abgerufen am 15.12.2017.

aus missbräuchlicher Verwendung der Credit Suisse TWINT-App durch unberechtigte Dritte ein unwiederbringlicher Schaden entstanden ist. Auch Credit Suisse schränkt die Entschädigung des Kunden dabei auf direkte Schäden und auf einen Maximalbetrag von CHF 5'000 ein (vgl. auch Ziff. 1.7 der Nutzungsbedingungen).[40]

b) Konstellation 1: Finder/Dieb bezahlt mit TWINT-App

Auf dieser Grundlage lässt sich die eingangs gestellte Frage nach der Schadentragung in der ersten Konstellation aus Sicht der Nutzer der TWINT-Apps aller drei TWINT-Issuer wie folgt beantworten: Der im Beispiel gewählte Code, welcher dem Jahrgang des Nutzers entspricht, stellt eine Sorgfaltspflichtverletzung des Nutzers dar, womit alle drei TWINT-Issuer eine Schadenübernahme aufgrund ihrer AGB ablehnen können und der Kunde den Schaden aus der nicht autorisierten Transaktion selbst zu tragen hat.

Hätte der Nutzer hingegen einen nicht leicht zu ermittelnden Code gewählt und entsprechend die diesbezüglichen Sorgfaltspflichten eingehalten, würden jedoch alle drei Issuer den entstandenen Schaden übernehmen. Anders als bei Raiffeisen ist diese Schadenübernahme bei TWINT AG und Credit Suisse allerdings auf den Maximalbetrag von CHF 5'000 beschränkt.

Ob der Nutzer sein Smartphone verliert (Konstellation 1 a) oder ob es ihm gestohlen wird (Konstellation 1 b), spielt in Zusammenhang mit der vertraglichen Beziehung zwischen Nutzer und TWINT-Issuer keine Rolle.

c) Konstellation 2: Fremde Kreditkarte/Bankkonto hinterlegt

Wird die TWINT-App (offensichtlich in betrügerischer Absicht) mit einer fremden Kreditkarte oder einem fremden Bankkonto hinterlegt, besteht zwischen der Person, deren Kreditkarten- bzw. Bankkonto mittels der unautorisierten Transaktion belastet wurde und dem jeweiligen TWINT-Issuer kein Vertragsverhältnis, weil diese Person die TWINT-App des TWINT-Issuers nicht heruntergeladen und dessen AGB entsprechend nicht akzeptiert hat. Da (in den meisten Fällen) auch keine andere Haftungsgrundlage ersichtlich ist, hat diese Person den Schaden nicht zu tragen.

40 Version 02/2017, abgerufen am 15.12.2017.

Der TWINT-Issuer, welcher innerhalb des Schemes den mit der TWINT-App «ausgegebenen» Betrag dennoch begleichen muss[41], hat einen Anspruch gegen den (allerdings wohl häufig unbekannten) Täter.

d) Konstellation 3: Mehrfachbelastung

Auch bei der dritten Konstellation handelt es sich letztlich um eine nicht autorisierte Transaktion. Der Nutzer hat für ein Grundgeschäft, beispielsweise den Kauf eines Buches, eine einmalige Transaktion in der Höhe des Kaufpreises für das Buch autorisiert. Die zweite (doppelte) Buchung hingegen hat er nicht autorisiert und entsprechend auch nicht zu bezahlen. Vorerst, d.h. im Verhältnis zwischen Nutzer und TWINT-Issuer, trägt der TWINT-Issuer diesen Schaden, sofern und soweit der Nutzer seine Sorgfaltspflichten eingehalten hat.

3. Scheme Rules

Die zweite Prüfungsstufe betrifft die Schadenverteilung zwischen Issuern, Acquirern und Scheme und stützt sich auf die Scheme Rules des TWINT-Zahlungssystems. Bei den einzelnen Regeln handelt es sich – wie bereits erwähnt – um Standardregeln, die in den gängigen Scheme Rules[42] weitestgehend gleich gehandhabt werden.

In der Konstellation 1, d.h. im Falle der Verwendung der TWINT-App durch eine nicht berechtigte Drittperson, kommt es im Verhältnis von Issuer, Acquirer und Scheme zur Schadensübernahme durch den Issuer. Wie die vorangehende Prüfungsstufe ergeben hat, wälzen die TWINT-Issuer einen solchen Schaden jedoch im Rahmen des Zahlungsdienstnutzungsvertrags bzw. der Nutzungsbedingungen regelmässig auf den TWINT-Nutzer ab.

Im Falle der Konstellationen 2 und 3, wenn der Schaden also nicht durch den Nutzer zu tragen ist, stellt sich die Frage, ob ein TWINT-Issuer diesen allenfalls auf den involvierten Acquirer oder das Scheme selbst (TWINT AG) abwälzen kann.

---

41 Vgl. unten.

42 Die Scheme Rules von MasterCard und VISA sind auf dem Internet veröffentlicht: <https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf> und <https://www.visaeurope.com/about-us/policy-and-regulation/veor>.

Wird mit einer TWINT-App eine fremde Kreditkarte bzw. ein fremdes Bankkonto verknüpft und anschliessend belastet (Konstellation 2), ist eine Abwälzung innerhalb des Schemes für den Issuer ausgeschlossen, weil in diesen Fällen die Scheme Rules generell die Haftung des Issuers vorsehen. Diese Regelung ist nachvollziehbar, weil es auch der Issuer ist, welcher die Nutzer in das Zahlungssystem einbindet und dabei entsprechend sorgfältig vorzugehen hat.

Demgegenüber haftet in der dritten Konstellation der jeweilige Acquirer. Das bedeutet, dass in jenen Fällen, in welchen dem TWINT-Nutzer der Transaktionsbetrag für dasselbe Grundgeschäft mehrfach belastet wurde, der doppelt geltend gemachte Betrag dem Issuer nicht belastet wird. Es versteht sich von selbst, dass die Acquirer in ihren Akzeptanzverträgen mit den Merchants für diesen Fall vorsehen, dass der entsprechende Betrag dem Merchantkonto nicht gutgeschrieben wird bzw. falls dies bereits geschehen ist, das Konto entsprechend wieder belastet wird. Auch diese Regelung ist angesichts der Tatsache, dass die Acquirer die Merchants in das Zahlungssystem einbinden, ohne weiteres nachvollziehbar.

4. Regulatorische Ebene

Schliesslich könnten in einer dritten Prüfungsebene gesetzliche bzw. regulatorische Vorgaben zu einer Veränderung der (vertraglichen) Schadenverteilung führen, wobei vorab an wettbewerbsrechtliche oder finanzmarktrechtliche Regeln zu denken ist.

In der Schweiz beschäftigt sich die Wettbewerbskommission (Weko) bereits seit mehr als zehn Jahren mit Zahlungssystemen, wobei der Fokus auf der *(domestischen) Interchange Fee*[43] sowie dem *Preisdifferenzierungsverbot*[44] lag.[45] Daneben stellte die Weko im Fall SIX/Terminals mit DCC die Markt-

[43] Interchange Fee oder Interbankenentgelt: Entgelt, das bei einem kartengebundenen Zahlungsvorgang für jede direkte oder indirekte (d.h. über einen Dritten vorgenommene) Transaktion zwischen dem Issuer und dem Acquirer gezahlt wird.

[44] Non-Discrimination-Rule, NDR: Scheme Regel, wonach die Zahlkarten des Schemes gegenüber anderen Zahlungsmethoden nicht diskriminiert werden dürfen (z.B. durch Preisaufschlag).

[45] Vgl. im Wesentlichen die folgenden Verfügungen der Weko: RPW 2003/1 S. 106 (NDR); RPW 2005/3 S. 530 (Rekurskommission); RPW 2007/1 S. 71 (NDR); RPW 2006/1 S. 65 (KKDMIF I, EVR I); RPW 2010/3 S. 473 (EVR II); RPW 2015/2 S. 165 (KKDMIF II, EVR III).

beherrschung auf den Acquiringmärkten fest.[46] Auch in Zusammenhang mit dem vorliegend interessierenden TWINT-Zahlungssystem wurde die Weko bereits aktiv und veröffentlichte eine begründete Stellungnahme zur Übernahme der TWINT AG durch die Postfinance AG und die SIX Payment Services AG.[47] Diese hat jedoch keinen Einfluss auf die vorliegend geprüfte Frage zur Schadenübernahme bei nicht autorisierten Transaktionen.

Auch die Finanzmarktgesetzgebung der Schweiz macht keine Vorgaben mit Bezug auf die vorliegend interessierende Schadenverteilung zwischen den am TWINT-Zahlungssystem beteiligten Parteien.

Anders die Regulierung im europäischen Ausland. Die Vorgaben der *PSD2*[48] mussten auf den 13. Januar 2018 in die nationalen Gesetze der EU-Mitgliedstaaten und der Länder des EWR übernommen werden. Unter vielen weiteren Vorgaben[49], enthält die PSD2 auch Vorgaben zur Verteilung der Haftung im Falle der unbefugten Verwendung von Zahlungsinstrumenten bzw. nicht autorisierten Transaktionen.

So haben die Mitgliedstaaten sicherzustellen, dass im Falle eines nicht autorisierten Zahlungsvorgangs der Zahlungsdienstleister (vorliegend: *Issuer*) des Zahlers diesem den Betrag eines nicht autorisierten Zahlungsvorgangs unverzüglich, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstags erstattet, nachdem er von dem Zahlungsvorgang Kenntnis erhalten hat oder dieser ihm angezeigt wurde. Dies ist nur dann nicht der Fall, wenn der Zahlungsdienstleister berechtigte Gründe für den Verdacht hat, dass Betrug vorliegt, und der zuständigen nationalen Behörde diese Gründe schriftlich mitteilt.[50]

Um dem Nutzer einen Anreiz zu geben, seinem Issuer jeden Diebstahl oder Verlust eines Zahlungsinstruments unverzüglich anzuzeigen und so das Risiko nicht autorisierter Zahlungsvorgänge zu verringern, soll der Nut-

46 RPW 2011/2 S. 96 (SIX/Terminals mit DCC).

47 RPW 2016/4 S. 1062 ff.

48 EU RL PSD II (Payment Services Directive) – Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25.11.2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. EU L 337/35 vom 23.12.2015).

49 Vgl. dazu den Beitrag von EMMENEGGER, Eckpunkte, S. 37 ff.

50 EU RL PSD II Art. 73 (1) und 74 (1).

zer für einen begrenzten Betrag (ca. EUR 50) selbst haften, auch wenn er alle Sorgfaltspflichten eingehalten oder leicht fahrlässig gehandelt hat.[51]

Weiter gibt die PSD 2 vor, dass die Aufteilung von Verlusten, die durch nicht autorisierte Zahlungsvorgänge verursacht werden, durch die nationalen Gesetze in den Mitgliedstaaten geregelt werden soll. So sollen beispielsweise der das Konto führende Zahlungsdienstleister und der in den Zahlungsvorgang eingebundene Zahlungsauslösedienstleister durch Haftungsverteilung gezwungen werden, für den jeweils von ihnen kontrollierten Teil des Zahlungsvorgangs die Verantwortung zu übernehmen.[52]

5. Fazit

TWINT ist ein rein schweizerisches Vier- bzw. Mehrparteien-Zahlungssystem und funktioniert im P2M-Bereich analog den entsprechenden, globalen Zahlungssystemen von MasterCard und Visa. Auch die Schadenverteilung für nicht autorisierte Transaktionen ist in allen drei Zahlungssystemen sehr ähnlich geregelt.

Die Haftungsverteilung zwischen Scheme, Issuern und Acquirern wird in den Scheme Rules, jene zwischen Issuern und Zahlern in den Zahlungsdienstnutzungsverträgen und jene zwischen Acquirern und Merchants in den Akzeptanzverträgen vorgenommen.

Der Nutzer der TWINT-App hat auf jeden Fall dann für Transaktionen einzustehen, welche er nicht autorisiert hat, wenn er die Sorgfaltspflichten im Umgang mit der App nicht eingehalten hat. Ist dies nicht der Fall, d.h. handelte der Nutzer sorgfältig, haftet er je nach TWINT-Issuer gar nicht oder nur für einen Schaden, der CHF 5'000 übersteigt.

51 EU RL PSD II Art. 74 (1).

52 EU RL PSD II Erwägung 73.

Literaturverzeichnis

ARTER OLIVER, Kreditkartenzahlungen im Fernabsatz, in: Jörg Florian S./Arter Oliver (Hrsg.), Internet-Recht und Electronic Commerce Law – 2. Tagungsband 2003, S. 267–327.

ARTER OLIVER/JÖRG FLORIAN S., Rückbelastungsklauseln bei Kreditkartenverträgen im E-Commerce, in: Schweizerische Juristen-Zeitung 2003, S. 25–34.

CUSTODIS HANS, Das Kreditkartenverfahren, Bankrechtliche Sonderveröffentlichungen des Instituts für Bankwirtschaft und Bankrecht an der Universität zu Köln, Bd. 11, Köln 1970.

EMMENEGGER SUSAN, PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 17–66.

GIGER HANS, Kreditkartensysteme – Eine ökonomisch-juristische Studie, Schriftenreihe zum Konsumentenschutzrecht, Bd. 17, Zürich 1985.

GOETZ STEFAN, Das internationale Kreditkartenverfahren, Schriftenreihe des Instituts für Internationales Recht und Internationale Beziehungen, Bd. 54, Basel 1992.

KELLER ALFRED, Kreditkarten – Ein praxisbezogener Leitfaden für Herausgeber von Kreditkarten und deren Vertragspartner, Juristen und Bankfachleute, Reihe zum Handels- und Wirtschaftsrecht, Bd. 15, Diessenhofen 1981.

KIENHOLZ GERFRIED, Die Zahlung mit Kreditkarte im Nah- und Fernabsatz, München 2000.

LANGENBUCHER KATJA, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, München 2001.

STENGEL CORNELIA/WEBER THOMAS, Digitale und mobile Zahlungssysteme – Technologie, Verträge und Regulation von Kreditkarten, Wallets und E-Geld, Zürich 2016.

WÜRSCH JOSEF, Die Kreditkarte nach schweizerischem Privatrecht – unter Berücksichtigung von Checkkarte und Bancomatkarte, Freiburg i.Ue. 1975.

Materialien

Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25.11.2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richt-linien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. EU L 337/35 vom 23.12.2015) – Payment Services Directive 25. November 2015.

Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (Amtsblatt der Europäischen Union L 123 vom 19.05.2015, S. 1) (Text von Bedeutung für den EWR) – Interchange Fee Regulation 29. April 2015.

Zahlung mit Bitcoins: Zahlung mit Sachen?

Bettina Hürlimann-Kaup, Freiburg*

Inhaltsverzeichnis

I. Einleitung

Bitcoins werfen in rechtlicher Hinsicht zahlreiche Fragen auf. Das gilt nicht nur für das Zivilrecht, sondern etwa auch für das Strafrecht, das Insolvenzrecht, das Bankenrecht und das Steuerrecht. Es erstaunt daher nicht, dass

* Ordentliche Professorin für Zivilrecht an der Universität Freiburg. Ich danke meiner Assistentin MLaw VANESSA M. FRESE für ihre Unterstützung bei der Erstellung dieses Beitrags. Prof. MIRJAM EGGEN, Universität Bern, danke ich für ihre hilfreichen Erläuterungen zur Funktionsweise der Bitcoins. – Das Manuskript wurde am 3. Mai 2018 abgeschlossen.

sich die Rechtswissenschaft bereits seit einiger Zeit intensiv mit den Bitcoins befasst. Insbesondere sind kürzlich einige Publikationen erschienen, die Bitcoins – im Widerspruch zur herrschenden Lehre – als Sachen im Sinn des Sachenrechts ansehen.[1] Diese Qualifizierung soll im Folgenden hinterfragt werden. Dazu wird zunächst in der gebotenen Kürze und damit notwendigerweise stark vereinfacht die Funktionsweise der Bitcoins vorgestellt (II.), bevor die These untersucht wird, Bitcoins liessen sich unter den Begriff der Sache subsumieren (III.). Den Abschluss bilden ein Fazit und ein Ausblick (IV.). Die Ausführungen beschränken sich auf das schweizerische Recht.

II. Funktionsweise der Bitcoins

«Bitcoin» bezeichnet einerseits ein dezentrales, durch Verschlüsselungstechnologie gesichertes Zahlungssystem, andererseits die Einheit dieses Systems:

– Beim *System* handelt es sich um ein sog. Peer-to-Peer-Netzwerk, d.h. jeder, der die Bitcoin-Software auf seinem Computer installiert, wird Teil des Netzwerks.[2] Es gibt keinen zentralen Server, sondern die Netzwerkteilnehmer sind direkt miteinander verbunden.[3]

  Zwei Hauptakteure prägen das Netzwerk, die Nutzer und die Miner.[4] Die Nutzer verwenden die Bitcoins als Zahlungssystem.[5] Dafür müssen sie über ein kryptografisches Schlüsselpaar verfügen: Aus dem Public Key lässt sich eine Bitcoin-Adresse (eine Art Kontonummer) ableiten. Mit dem Private Key (eine Art Passwort) kann eine Transaktion signiert bzw. vom Empfänger dekodiert werden. Das Schlüsselpaar ist regelmässig in einer Wallet (eine Art digitale Brieftasche) abgespeichert, die ausserdem angibt, über wie viele Bitcoins der Nutzer gegenwärtig verfügt.[6] Um eine Transaktion durchzuführen, geben die Nutzer einen entsprechenden Auftrag an das Netzwerk. Die Miner wickeln die aufgegebenen Aufträge ab, indem sie durch die Lösung komplexer mathematischer Gleichungen

---

1 Vgl. namentlich den Beitrag von GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology; LINDER/MEYER, Steuerliche Behandlung, S. 197 f.; sowie (mit Bezug auf digitale Daten allgemein) den Aufsatz von ECKERT, Digitale Daten als Sache.

2 GLESS/KUGLER/STAGNO, Geld, S. 86.

3 JACQUEMART/MEYER, Hardfork, S. 470.

4 Vgl. zum Folgenden auch den Bericht des Bundesrates zu virtuellen Währungen, S. 8.

5 GLESS/KUGLER/STAGNO, Geld, S. 86.

6 JACQUEMART/MEYER, Hardfork, S. 471; MIGNON, Le « [B]itcoin », Rz 8.

bestätigen, dass dem Auftraggeber die erforderliche Anzahl von Bitcoins tatsächlich zukommt und er nicht schon früher einmal darüber verfügt hat.[7] Um diese Gleichungen zu berechnen, ist eine enorme Rechenleistung erforderlich. Bestätigte Transaktionen werden in chronologischer Reihenfolge ca. alle 10 Minuten zu einem Block zusammengefasst und an die Kette der bereits bestehenden Transaktionen angehängt.[8] Bei dieser sog. Blockchain handelt es sich also um eine Art Kontobuch, das alle jemals getätigten Transaktionen wiedergibt. Sie ist weltweit auf unzähligen Hard Disks gespeichert und wird ständig aktualisiert.[9]

Die Miner werden für ihre Rechenleistung belohnt, indem ihnen eine bestimmte Anzahl an Bitcoins gutgeschrieben wird, welche ihre Computer durch die Lösung der sich stellenden mathematischen Probleme im Moment neu generieren.[10] Es gibt mit anderen Worten keinen zentralen Emittenten, der Bitcoins herausgibt und in irgendeiner Form steuernd eingreift.[11] Ein Nutzer hat weder gegenüber dem Netzwerk noch gegenüber den Minern oder den anderen Nutzern eine Forderung.[12]

– Der Bitcoin als *Einheit* dieses Systems einer virtuellen Währung ist ein Vermögenswert, der bloss als digitaler Code existiert,[13] und zwar als Kette digitaler Signaturen, die auf der Blockchain gespeichert ist.[14]

---

7 PILLER, Virtuelle Währungen, S. 1427; GLESS/KUGLER/STAGNO, Geld, S. 87.

8 GOBAT, Les monnaies virtuelles, S. 1097.

9 MEISSER, Kryptowährungen, S. 83 f.; WEBER, Blockchain, Rz 2.

10 GLESS/KUGLER/STAGNO, Geld, S. 87; MEISSER, Kryptowährungen, S. 86 f. Das gilt nur so lange, bis die maximale Anzahl Bitcoins von 21 Millionen erreicht ist; vgl. dazu MEISSER, Kryptowährungen, S. 87. Zusätzlich zu den Bitcoins erhält der Miner für jeden von ihm geminten Block alle Transaktionsgebühren, die den im Block enthaltenen Aufträgen beigefügt worden sind. Die Höhe der Gebühr wird vom jeweiligen Nutzer selbst (allenfalls auch von den Nutzungsbedingungen der Wallet-Software) festgelegt. Allgemein gilt: Je höher die ausgewiesene Gebühr, desto eher ist mit einer Bestätigung durch die Miner zu rechnen; vgl. zum Ganzen SIXT, Bitcoins, S. 101.

11 MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 21.

12 PILLER, Virtuelle Währungen, S. 1428; MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 21; GOBAT, Les monnaies virtuelles, S. 1098.

13 Bericht des Bundesrates zu virtuellen Währungen, S. 8.

14 JACQUEMART/MEYER, Hardfork, S. 471. – Entgegen einer landläufigen Meinung sind die Bitcoins nicht in der Wallet des jeweiligen Nutzers vorhanden. Soll der Saldo einer bestimmten Bitcoin-Adresse berechnet werden, muss das über die Blockchain geschehen; vgl. MIGNON, Le « [B]itcoin », Rz 8; HARI, La revendication, S. 455.

III. Bitcoins als Sachen?

1. Begriff der Sache

Das ZGB umschreibt den Begriff der Sache nicht. Nach der ganz überwiegenden Lehre müssen Objekte *vier Merkmale* aufweisen, um Sachen im Sinn des Sachenrechts zu sein: die Unpersönlichkeit, die Körperlichkeit, die Abgegrenztheit und die rechtliche Beherrschbarkeit.[15] Bitcoins sind nach dem soeben Gesagten lediglich digitale Codes. Damit erfüllen sie weder das Merkmal der Körperlichkeit noch dasjenige der Abgegrenztheit, bei dem es um die Abgegrenztheit «im Raum» geht[16].

Diejenigen Autoren, die Bitcoins dennoch als Sachen qualifizieren, ziehen unter anderem *Art. 713 ZGB* als Argument dafür heran, dass auch etwas Unkörperliches den Sachbegriff erfüllen kann.[17] Die Norm, die den Gegenstand des Fahrniseigentums umschreibt, hat folgenden Wortlaut:

> «Gegenstand des Fahrniseigentums sind die ihrer Natur nach beweglichen körperlichen Sachen sowie die Naturkräfte, die der rechtlichen Herrschaft unterworfen werden können und nicht zu den Grundstücken gehören.»

Nicht nur an beweglichen Sachen, sondern auch an bestimmten Naturkräften können also kraft ausdrücklicher gesetzlicher Anordnung Eigentumsrechte bestehen. Die überwiegende Lehre spricht diesen Naturkräften (in Übereinstimmung mit dem Gesetz) die Körperlichkeit und damit die Sachqualität ab.[18] Es gibt aber auch Stimmen in der Literatur, welche die Körperlichkeit unter Hinweis auf heutige wissenschaftliche Erkenntnisse bejahen.[19] Einigkeit besteht immerhin darüber, dass die sachenrechtlichen Normen wegen der Besonderheiten der Naturkräfte *nur analoge Anwendung* finden

---

15 Vgl. statt vieler SCHMID/HÜRLIMANN-KAUP, Sachenrecht, Nr. 4 ff. mit Hinweisen.

16 BK ZGB-MEIER-HAYOZ, Syst. Teil N 120; BSK ZGB-WIEGAND, Vorbem. zu Art. 641 ff. N 8; REY, Grundlagen, Nr. 69; STEINAUER, Band I, Nr. 63.

17 Vgl. insbesondere GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 43 f. und 51.

18 Vgl. etwa BSK ZGB-WIEGAND, Vorbem. zu Art. 641 ff. N 14; STEINAUER, Band I, Nr. 114; SCHMID/HÜRLIMANN-KAUP, Sachenrecht, Nr. 7.

19 So insbesondere BK ZGB-MEIER-HAYOZ, Syst. Teil N 225. Auch nach Ansicht von REY, Grundlagen, Nr. 86, kann der Energie die Körperlichkeit nicht vollständig abgesprochen werden.

können.[20] Die Bestimmung eignet sich damit nicht dazu, die Sachqualität von Bitcoins zu begründen.

Die *Körperlichkeit* ist das *zentrale Merkmal* des Sachbegriffs,[21] was sich bereits darin zeigt, dass das Sachenrecht des ZGB ganz überwiegend auf körperlich greifbare Güter ausgerichtet ist.[22] Nach der hier vertretenen Ansicht ist es schon aus diesem Grund de lege lata ausgeschlossen, Bitcoins unter den Sachbegriff zu subsumieren. Daran ändert auch die sog. Funktionalität des Sachbegriffs nichts,[23] wonach nicht allein die physikalische Beschaffenheit, sondern vor allem die wirtschaftliche Funktion, die Verkehrsanschauung und ethische Gesichtspunkte dafür ausschlaggebend sind, ob ein Objekt eine Sache darstellt.[24] Auf die Voraussetzung der Körperlichkeit wird also keineswegs verzichtet, vielmehr werden zusätzliche Kriterien herangezogen, um ein (körperliches) Objekt rechtlich zu qualifizieren.[25]

2. Anwendbarkeit sachenrechtlicher Normen?

Einzelne Autoren sprechen sich für eine «zeitgemässe Interpretation» des Sachbegriffs aus und halten anstelle des als zu starr empfundenen Merkmals

---

20 Vgl. statt vieler BK ZGB-MEIER-HAYOZ, Syst. Teil N 226; REY, Grundlagen, Nr. 86. So lässt sich bei Naturkräften zum Beispiel kaum von Besitz sprechen; STEINAUER, Band II, Nr. 1987a.

21 BSK ZGB-WIEGAND, Vorbem. zu Art. 641 ff. N 10.

22 Ausnahmsweise lässt das Gesetz dingliche Rechte an unkörperlichen Gütern zu und stellt diese insofern den Sachen gleich (vgl. insbesondere Art. 655 Abs. 2 Ziff. 2 und 4, 745 Abs. 1 und 773 ff., 899 ff. ZGB).

23 So aber GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 44, 68 und 115.

24 Vgl. zum Ganzen BK ZGB-MEIER-HAYOZ, Syst. Teil N 116; BSK ZGB-WIEGAND, Vorbem. zu Art. 641 ff. N 6; REY, Grundlagen, Nr. 68. Etwas anders GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 44 und 115, nach deren Auffassung Bitcoins Gegenstand von Eigentumsrechten sein können, sofern die wirtschaftliche Funktion, die Verkehrsanschauung und ethische Gesichtspunkte *nicht dagegen sprechen* (wie hier allerdings Rz 43).

25 Bei den in der Lehre in diesem Zusammenhang genannten Beispielen ist die Körperlichkeit denn auch stets gegeben, soweit es um das geltende Recht geht; vgl. etwa REY, Grundlagen, Nr. 68 und 119: Frage nach der Sachqualität eines Bienenschwarms bzw. eines Embryos in vitro. Anders nun aber GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 43 f. und 115. – Zu Überlegungen hinsichtlich elektronischer und biotechnischer Gegenstände *de lege ferenda* vgl. BSK ZGB-WIEGAND, Vorbem. zu Art. 641 ff. N 6.

der Körperlichkeit dasjenige der ausschliesslichen Beherrschbarkeit für massgebend.[26] Wären Bitcoins tatsächlich als Sachen zu qualifizieren, fänden auf sie die sachenrechtlichen Normen Anwendung. Was das bedeuten würde, soll im Folgenden beispielhaft anhand des Inhalts (a.) und der Übertragung des Eigentums (b.) untersucht werden.

a) Inhalt des Eigentums

Art. 641 ZGB unterscheidet zwischen der positiven und der negativen Seite des Eigentumsrechts:

– Die *positive Seite* (Abs. 1) umfasst unter anderem die tatsächliche und rechtliche Verfügungsmacht über die Sache.[27] Für digitale Daten folgt daraus das Recht des Inhabers, über das Kopieren, Reproduzieren oder Multiplizieren seiner Daten zu bestimmen.[28] Dass das bei Bitcoins nicht der Fall sein kann, versteht sich auf Grund der Funktionsweise der Blockchain von selbst.[29]

  Die Verfügungsmacht beinhaltet weiter das grundsätzliche Recht des Eigentümers, die Sache zu zerstören.[30] Auch dieses Recht fällt bei den Bitcoins ausser Betracht: Die einzige Möglichkeit, die der Berechtigte hat, ist die Zerstörung des Private Key. Damit ist ein Zugriff auf die betroffenen Bitcoins zwar für immer ausgeschlossen,[31] der entsprechende digitale Code besteht aber nach wie vor.[32]

  Der Berechtigte kann immerhin mithilfe seines Private Key Bitcoins auf Dritte übertragen. Dieses Recht gilt allerdings nach dem Gesagten[33] nicht voraussetzungslos, sondern ist davon abhängig, dass die Miner die Transaktion validieren.[34]

---

26 LINDER/MEYER, Steuerliche Behandlung, S. 198.

27 Vgl. statt vieler BK ZGB-MEIER-HAYOZ, Art. 641 N 26 und 28.

28 ECKERT, Besitz und Eigentum, S. 271. Nach HAUSER-SPÜHLER/MEISSER, Eigenschaften, S. 9, ist allerdings zweifelhaft, ob sich Bitcoins rechtlich als Daten qualifizieren lassen.

29 Vgl. auch GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 67.

30 Vgl. statt vieler BK ZGB-MEIER-HAYOZ, Art. 641 N 27.

31 ESSEBIER/WYSS, Blockchain, Rz 23.

32 HARI, La revendication, S. 454 f.

33 Oben II.

34 Transaktionen, bei denen nur eine sehr kleine oder gar keine Transaktionsgebühr vorgesehen ist, werden unter Umständen von den Minern überhaupt nicht bearbeitet; SIXT, Bitcoins, S. 96. – Zum Risiko einer «51-Prozent-Attacke», bei der ein Minerpool,

– Die *negative Seite* (Abs. 2) betrifft den absoluten Schutz des Eigentümers gegenüber Dritten. Insbesondere hat der Eigentümer das Recht, mit der Rei vindicatio die Sache von jedem herauszuverlangen, der sie ihm ohne Rechtsgrund vorenthält.[35] Eine solche Situation wäre im vorliegenden Zusammenhang zum Beispiel gegeben, wenn eine Drittperson einem Nutzer den Private Key entwenden und damit Bitcoins an ihre eigene Adresse transferieren würde. Ziel der Rei vindicatio ist die «Übertragung des unmittelbaren Besitzes an der Sache auf den Eigentümer»[36]. Das scheitert hier m.E. bereits daran, dass ein Besitz an Bitcoins nicht möglich ist (siehe dazu unten b./bb.). Darüber hinaus kann eine Transaktion, sobald sie in die Blockchain aufgenommen worden ist, vom einzelnen Nutzer nicht mehr rückgängig gemacht werden.[37] In Betracht käme lediglich eine Rückübertragung oder die Herausgabe des Private Key.[38]

Aus dem Gesagten ergibt sich, dass der berechtigten Person bei Bitcoins *wesentliche aus Art. 641 ZGB fliessende Rechte nicht zukommen* können.

b) Übertragung des Eigentums

Zu untersuchen ist im Folgenden der derivative Eigentumserwerb, geht es doch regelmässig um die Konstellation, dass ein Nutzer einem anderen eine bestimmte Anzahl von Bitcoins überweist. Für den Eigentumserwerb bedarf es eines Verpflichtungs- und eines Verfügungsgeschäfts:

aa) Verpflichtungsgeschäft

Gemäss dem im Sachenrecht geltenden *Kausalitätsprinzip* muss das Verpflichtungsgeschäft gültig sein, damit das Eigentum auf den Erwerber übergeht.[39] Ist im konkreten Fall der Vertrag, welcher der Überweisung der Bitcoins zugrunde liegt, etwa wegen Urteilsunfähigkeit einer Partei ungültig, hat der Empfänger das Eigentum nicht erworben. Dem Veräusserer steht

---

der 51% der Miner-Rechenleistung beherrscht, die Bestätigung bestimmter oder aller Transaktionen verhindern kann, vgl. SIXT, Bitcoins, S. 105 f.

35 Vgl. statt vieler BK ZGB-MEIER-HAYOZ, Art. 641 N 32.

36 BK ZGB-MEIER-HAYOZ, Art. 641 N 61.

37 ESSEBIER/WYSS, Blockchain, Rz 4 und 10.

38 MEYER/SCHUPPLI, «Smart Contracts», S. 220.

39 Vgl. statt aller SCHMID/HÜRLIMANN-KAUP, Sachenrecht, Nr. 75.

aber, wie soeben dargelegt, nicht die Möglichkeit offen, mit der Rei vindicatio die Herausgabe der Bitcoins zu verlangen.

Fällt ein derivativer Eigentumserwerb auf Grund der Ungültigkeit des Rechtsgrunds ausser Betracht, bleibt zu prüfen, ob stattdessen ein *originärer Erwerb* erfolgt ist:

– Zu untersuchen ist zunächst die Möglichkeit einer *Vermischung,* wie sie bei Geldscheinen oder -münzen vorkommt.[40] Hier wird der Besitzer nach bundesgerichtlicher Rechtsprechung originär Eigentümer des Geldes, wenn sich wegen der Vermischung der Scheine oder Münzen nicht mehr feststellen lässt, von wem welches Geld stammt.[41] Eine solche Vermischung fällt für den vorliegenden Fall ausser Betracht, da alle Bitcoins auf Grund ihrer Signaturkette individuell bestimmbar sind.[42]
– Weiter stellt sich die Frage nach einem originären Eigentumserwerb für den Fall, dass die auf Grund eines ungültigen Verpflichtungsgeschäfts transferierten Bitcoins bereits auf einen gutgläubigen Dritten weiter übertragen worden sind.[43] Bei beweglichen Sachen ist im Fall eines Erwerbs des Besitzes von einem Nichtberechtigten ein *Gutglaubensschutz nach Art. 933 ZGB* gegeben, wenn der ursprüngliche Besitzer die Sache dem Veräusserer «anvertraut» hat. Diese Voraussetzung ist auch dann erfüllt, wenn der Besitz des Veräusserers auf einem ungültigen Vertrag beruht.[44] Der Grund für den Gutglaubensschutz liegt hier darin, dass der frühere Besitzer den falschen Rechtsschein[45] selbst gesetzt hat, weshalb er nach Wertung des Gesetzgebers weniger schutzwürdig ist als der Dritte.[46] Nach der hier vertretenen Ansicht lässt sich bei den Bitcoins aber nicht von einer solchen Rechtsscheinsituation sprechen, da keine

---

40 Zur Frage, ob Bitcoins Geldcharakter haben, vgl. etwa den Bericht des Bundesrates zu virtuellen Währungen, S. 7 f.; MEYER/SCHUPPLI, «Smart Contracts», S. 220; BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 143 f.

41 Grundlegend BGE 47 II 267 E. 2 S. 270 f. Vgl. etwa auch BGE 116 IV 193 E. 4 S. 201 f.; 136 III 247 E. 5 S. 252.

42 MEYER/SCHUPPLI, «Smart Contracts», S. 220. Ebenso (mit etwas anderer Begründung) LINDER/MEYER, Steuerliche Behandlung, S. 199.

43 Die folgenden Ausführungen stehen unter der Prämisse, dass Besitz an Bitcoins möglich ist (siehe aber sogleich bb.).

44 BK ZGB-STARK/LINDENMANN, Art. 933 N 24 und 29 ff.

45 Vgl. Art. 930 Abs. 1 ZGB: «Vom Besitzer einer beweglichen Sache wird vermutet, dass er ihr Eigentümer sei».

46 Vgl. statt vieler BK ZGB-STARK/LINDENMANN, Art. 933 N 22.

Transaktion zwischen eindeutig identifizierten Parteien hinsichtlich eines eindeutig zuzuordnenden Objekts vorliegt, sondern ein weitestgehend anonymisiertes System von Transaktionen. Es fehlt also an einer «sinnlich wahrnehmbare[n] tatsächliche[n] Inhaberschaft des Veräusserers an der Sache»[47], von der Art. 933 ZGB ausgeht.[48]

Anerkennt man bei den Bitcoins dennoch eine Rechtsscheinsituation, stellt sich sogleich die Frage nach dem guten Glauben. Bei Bitcoins darf als allgemein bekannt vorausgesetzt werden, dass durch Hackerangriffe immer wieder Private Keys entwendet werden und den Nutzern dadurch hohe Beträge verloren gehen.[49] Es ist zumindest fraglich, ob der Empfänger von Bitcoins unter diesen Umständen grundsätzlich als gutgläubig angesehen werden kann oder ob er nicht vielmehr eine erhöhte Erkundigungspflicht hätte (vgl. Art. 3 Abs. 2 ZGB). Wäre das zu bejahen, bliebe das Problem, wie einer solchen Pflicht in diesem anonymisierten System überhaupt nachzukommen wäre.

Aus dem Gesagten folgt, dass *Art. 933 ZGB auf die Situation der Bitcoins nicht zugeschnitten* ist.

Insgesamt gesehen ist *fraglich, ob das Kausalitätsprinzip* im Zusammenhang mit Bitcoins *zu einer angemessenen Lösung führt.*[50]

---

47 ROTH, Zukunft des Wertpapierrechts, S. 179.

48 Die Situation hinsichtlich der Bitcoins ähnelt derjenigen bei den Bucheffekten, bei denen es ebenfalls um ein anonymisiertes Massengeschäft geht. Art. 29 Abs. 1 BEG sieht unter bestimmten Voraussetzungen zwar einen Gutglaubensschutz vor, aber nicht, weil der ursprünglich Berechtigte durch eine Besitzübertragung einen falschen Rechtsschein gesetzt hätte. Vielmehr geht es darum, das Vertrauen in das Verwahrungs- und Abwicklungssystem und damit den Rechtsverkehr zu schützen; DAENIKER/LEISINGER, Kommentar zum BEG, Art. 29 BEG N 8 und 30; vgl. auch ROTH, Zukunft des Wertpapierrechts, S. 180 f.; KUHN, Kreditsicherungsrecht, § 26 N 83. Die Ratio von Art. 29 Abs. 1 BEG ist damit nicht identisch mit derjenigen von Art. 933 ZGB. Vgl. auch die Botschaft zum BEG, S. 9332, wonach die sachenrechtlichen Gutglaubensregeln (Art. 933 ff. ZGB) für die mediatisierte Wertpapierverwahrung untauglich sind.

49 Vgl. dazu den Bericht des Bundesrates zu virtuellen Währungen, S. 21; SIXT, Bitcoins, S. 92 ff.

50 GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 43, scheinen die Anwendbarkeit des Kausalitätsprinzips in diesem Zusammenhang für unproblematisch zu halten, ohne allerdings auf die Frage nach der Rechtsfolge im Fall eines ungültigen Verpflichtungsgeschäfts einzugehen. – Eine ähnliche Situation wie bei den Bitcoins zeigt sich bei der Übertragung von Bucheffekten im Sinn einer Gutschrift nach Art. 24 BEG. Bei den Bucheffekten, bei denen es sich unbestrittenermassen nicht um Sachen handelt (vgl. nur schon die Botschaft zum BEG, S. 9339), gilt nach wohl über-

bb) Verfügungsgeschäft

Der Eigentumsübergang setzt (neben dem gültigen Verpflichtungsgeschäft) die *Besitzübertragung* auf den Erwerber voraus (Art. 714 Abs. 1 ZGB; Verfügungsgeschäft). Art. 919 Abs. 1 ZGB umschreibt den Besitz als die tatsächliche Gewalt über die Sache. Bei Bitcoins lässt sich mangels Körperlichkeit kaum von Besitz sprechen.[51] Insbesondere lässt sich nicht sagen, der Besitzer der Bitcoins sei der Besitzer der Hard Disk, auf der die Transaktion gespeichert ist, weil es sich bei der Blockchain nach dem Gesagten[52] um ein dezentrales Netzwerk handelt und die Information damit auf unzähligen Hard Disks vorhanden ist.

In der Lehre gibt es Stimmen, die den Besitz derjenigen Person zusprechen wollen, die über den entsprechenden *Private Key* verfügt.[53] Dieser ist zwar Voraussetzung dafür, dass die Bitcoins übertragen werden können, er reicht für sich allein aber nicht aus, da eine Transaktion, wie oben[54] dargelegt, nur dann in die Blockchain aufgenommen wird, wenn die Miner sie validiert haben.[55]

Für die folgenden Überlegungen wird dennoch angenommen, durch den Private Key sei Besitz gegeben: Die Besitzübertragung kann dadurch erfolgen, dass der Veräusserer dem Erwerber Zugriff auf sein Konto gibt, indem er ihm seinen Private Key mitteilt.[56] Im Normalfall wird die Übertragung aber durch eine Überweisung vorgenommen. Der Nutzer signiert zu diesem Zweck die Transaktion mit seinem Private Key. Ausserdem muss ihm die

---

wiegender Lehre nicht das Kausalitäts-, sondern das Abstraktionsprinzip; vgl. etwa KUHN, Kreditsicherungsrecht, § 26 N 57 mit Hinweisen. Begründet wird dies mit dem Verkehrsschutz; BÄRTSCHI, Rechtliche Umsetzung, S. 1078, Fn. 65. Fehlt es an einer gültigen Causa, erfolgt die Rückabwicklung nach schuldrechtlichen Grundsätzen; ZOBL/GERICKE, Kommentar zum BEG, Syst. Teil N 99 ff. unter Hinweis auf BGE 138 III 137 E. 5.2.1 S. 140.

51 Vgl. dazu auch WEBER/THOUVENIN, Dateneigentum, S. 49.

52 Oben II.

53 ECKERT, Besitz und Eigentum, S. 266.

54 Vgl. II.

55 Im Übrigen ist auch mit Bezug auf Bucheffekten Besitz zu verneinen. Vgl. dazu bereits die Botschaft zum BEG, S. 9378: «Die Besitzesschutzregeln knüpfen an den Besitz einer Sache an; eine Vorstellung, die bei der mediatisierten Wertpapierverwahrung nicht zutrifft.».

56 MEISSER, Kryptowährungen, S. 85; BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 147 und 149 f.

Bitcoin-Adresse des Empfängers bekannt sein. Bei der Transaktion findet kein Übergang von Daten statt, sondern es wird an den als Kette digitaler Signaturen definierten Bitcoin eine neue Signatur angehängt.[57] Nach Art. 923 ZGB wäre die Besitzübertragung in dem Moment abgeschlossen, in dem der Empfänger die signierte Transaktion erhalten hat. Bei der Übertragung von Bitcoins handelt es sich aber um einen graduellen Prozess.[58] Im Zeitpunkt des Eintreffens der signierten Transaktion beim Empfänger ist diese im Netzwerk noch nicht bekannt. Während einer (allenfalls nur sehr kurzen Zeit) können Sender und Empfänger beide über die Bitcoins verfügen.[59] Üblicherweise wird die Zahlung im Moment der Veröffentlichung akzeptiert, wenn also eine Mehrheit der Netzwerkteilnehmer über die Transaktion informiert ist.[60] Bei grösseren Beträgen akzeptiert der Empfänger die Zahlung häufig erst, wenn an den Block, der die Transaktion enthält, eine bestimmte Anzahl weiterer Blöcke angehängt worden ist. Je tiefer die Transaktion in der Blockchain liegt, desto sicherer kann der Erwerber nämlich sein, dass sie von den Minern nicht mehr rückgängig gemacht wird.[61] Dass der Zeitpunkt des Besitzübergangs (wie hier) vom Willen der Parteien abhängt, kennt das Sachenrecht im Fall des Traditionssurrogats der Besitzanweisung (vgl. Art. 924 ZGB), also wenn sich die Sache im unmittelbaren Besitz eines Dritten befindet und Veräusserer und Erwerber den Besitz durch die Besitzanweisung auf den gewünschten Zeitpunkt hin übertragen.[62] Die Konstellation eines Dreiparteienverhältnisses ist bei den Bitcoins aber gerade nicht gegeben.

Zusammenfassend ergibt sich, dass an Bitcoins *kein Besitz* bestehen kann.

---

57 MEYER/SCHUPPLI, «Smart Contracts», S. 220; MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 7; GOBAT, Les monnaies virtuelles, S. 1096 f.; JACQUEMART/MEYER, Hardfork, S. 471.

58 BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 148, Fn. 109.

59 MEISSER, Kryptowährungen, S. 85.

60 MEISSER, Kryptowährungen, S. 85.

61 MEISSER, Kryptowährungen, S. 84 f. und 86; SIXT, Bitcoins, S. 99.

62 Vgl. etwa SCHMID/HÜRLIMANN-KAUP, Sachenrecht, Nr. 170.

IV. Fazit und Ausblick

Die vorstehenden Ausführungen haben Folgendes gezeigt:

- Die Bitcoins erfüllen zwei der vier Merkmale des Sachbegriffs nicht.
- Weder besteht die rechtliche und tatsächliche Verfügungsmacht noch der Anspruch auf Herausgabe, wie in Art. 641 ZGB vorgesehen.
- Es ist zweifelhaft, ob die Anwendung des Kausalitätsprinzips auf die Bitcoins angemessen ist.
- Besitz im Sinn der tatsächlichen Gewalt über die Sache ist bei Bitcoins nicht möglich.

Daraus ergibt sich ohne Weiteres, dass *Bitcoins keine Sachen* im Sinn des Sachenrechts sein können.[63]

Es bleibt die Frage, warum ein Teil der Lehre die gegenteilige Meinung vertritt,[64] obwohl die sachenrechtlichen Bestimmungen auf die Bitcoins ganz offensichtlich nicht passen. Der Grund dafür scheint in erster Linie im *Insolvenzrecht* zu liegen.[65] Viele Personen loggen sich nicht selbst in das Bitcoin-Netzwerk ein, sondern nutzen spezifische Webseiten, die unter anderem die Verwahrung von Bitcoins anbieten.[66] Geht ein solcher Dienstleister Konkurs und fallen die durch ihn verwahrten Bitcoins in seine Konkursmasse, stellt sich die Frage, ob der Nutzer gestützt auf *Art. 242 SchKG* ein Aussonderungsrecht hat.[67] Nach Abs. 1 dieser Norm trifft die Konkursverwaltung «ei-

---

63 Die Sachqualität ebenfalls verneinend BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 141; GOBAT, Les monnaies virtuelles, S. 1098 und 1101; MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 20; PILLER, Virtuelle Währungen, S. 1429 und 1438; HAUSER-SPÜHLER/MEISSER, Eigenschaften, S. 10. Ebenso mit Bezug auf Daten allgemein HÜRLIMANN/ZECH, Rechte an Daten, S. 92, Ziff. 8.

64 Vgl. GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 58 ff.; LINDER/MEYER, Steuerliche Behandlung, S. 198; HARI, La revendication, S. 465. In diese Richtung auch SCHÖNKNECHT, Einlagebegriff, S. 310, Fn. 90.

65 Vgl. etwa GRAHAM-SIEGENTHALER/FURRER, Position of Blockchain Technology, Rz 11 und 71; HARI, La revendication, S. 466.

66 Vgl. zu den typisierten Grundformen der Verwahrung von Bitcoins MAURENBRECHER/-MEIER, Insolvenzrechtlicher Schutz, Rz 9 ff. Vgl. ausserdem JACQUEMART/MEYER, Hardfork, S. 478.

67 Ein entsprechendes Problem stellt sich mit Bezug auf die Absonderung im Konkurs einer Bank; vgl. Art. 37d i.V.m. Art. 16 BankG. Zur Frage, wann im Zusammenhang mit Bitcoins Einlagen im bankenrechtlichen Sinn vorliegen, vgl. den Bericht des Bundesrates zu virtuellen Währungen, S. 13 f.; EFD, Änderung des Bankengesetzes, S. 15;

ne Verfügung über die Herausgabe von Sachen, welche von einem Dritten beansprucht werden». Das Bundesgericht lehnt es in konstanter Rechtsprechung ab, Forderungen, die nicht in einem Wertpapier verkörpert sind, unter den Begriff der Sache im Sinn von Art. 242 Abs. 1 SchKG zu subsumieren.[68] Da aber das Gericht gerade auf das Erfordernis der Körperlichkeit abstellt,[69] lässt sich eine Aussonderung der Bitcoins von vorneherein nicht über die Ausdehnung des Sachbegriffs auf unkörperliche Objekte erreichen.[70] Es ist vielmehr eine Frage des Insolvenzrechts, ob sich de lege lata eine analoge Anwendung von Art. 242 SchKG auf die Bitcoins rechtfertigt[71] oder ob dafür eine Änderung des SchKG erforderlich ist.

Zurzeit ist im Nationalrat eine Parlamentarische Initiative[72] hängig, die folgende Ergänzung von Art. 242 SchKG verlangt:

> «Die Konkursverwaltung trifft eine Verfügung über die Herausgabe von nichtkörperlichen Vermögenswerten, welche von einem Dritten beansprucht werden. Die Herausgabe setzt voraus, dass die nichtkörperlichen Vermögenswerte separiert werden können und der Antragsteller glaubhaft machen kann, dass diese dem Schuldner nur anvertraut sind. Die anfallenden Kosten sind vom Antragssteller zu tragen.»

FINMA, Unerlaubt tätige Finanzmarktanbieter, S. 15. Vgl. ausserdem MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 29 ff.

68 Vgl. BGE 128 III 388 S. 388 f. mit Hinweisen; anders immerhin BGE 39 I 129 E. 1 S. 131.

69 Vgl. etwa BGE 70 III 34 S. 37: «bien corporel»; 76 III 9 E. 1 S. 10: «körperliche Sachen»; 105 III 11 E. 2 S. 14: «nicht in einem Wertpapier verkörperte Forderung»; 128 III 388 S. 389: «créance inventoriée non incorporée dans un titre».

70 So aber ECKERT, Besitz und Eigentum, S. 272.

71 Vgl. auch WEBER/THOUVENIN, Dateneigentum, S. 58. Die Anwendbarkeit gestützt auf die bundesgerichtliche Rechtsprechung verneinend PILLER, Virtuelle Währungen, S. 1437. In der Tendenz für gewisse Konstellationen bejahend MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 26 («funktionale Auslegung von Art. 242 SchKG»); vgl. auch HAUSER-SPÜHLER/MEISSER, Eigenschaften, S. 10 ff. GRAHAM-SIEGENTHALER/-FURRER, Position of Blockchain Technology, Rz 92, begründen die Zulässigkeit der Aussonderung von Bitcoins gestützt auf Art. 242 Abs. 1 SchKG unter anderem mit deren Ähnlichkeit mit den Bucheffekten, die ihrerseits gestützt auf die ausdrückliche Anordnung in Art. 29 Abs. 3 BEG im Konkurs eines rückerstattungspflichtigen Erwerbers aussonderbar sind.

72 Parlamentarische Initiative Nr. 17.410 vom 7. März 2017 (NR MARCEL DOBLER): Daten sind das höchste Gut privater Unternehmen. Datenherausgabe beim Konkurs von Providern regeln. Die Kommission für Rechtsfragen des Nationalrats hat der parlamentarischen Initiative am 3. Mai 2018 Folge gegeben.

Ob eine Änderung von Art. 242 SchKG im beschriebenen Sinn genügt[73] oder ob mit Bezug auf virtuelle Währungen allenfalls – wie seinerzeit bei den Bucheffekten – ein neues absolutes Recht zu schaffen ist,[74] muss der Gesetzgeber entscheiden. Der Bundesrat hat angekündigt, die rechtliche Qualifikation der Bitcoins klären zu wollen.[75] Diese wird wohl im grösseren Rahmen der Einordnung digitaler Daten vorgenommen werden müssen.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 3. Mai 2018.

BÄRTSCHI HARALD, Die rechtliche Umsetzung des Bucheffektengesetzes, AJP 2009, S. 1071–1087.

BÄRTSCHI HARALD/MEISSER CHRISTIAN, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich/Basel/Genf 2015 (ZIK Band 61), S. 113–160.

DAENIKER DANIEL/LEISINGER BENJAMIN, Art. 29 BEG, in: Zobl Dieter/Hess Martin/Schott Ansgar (Hrsg.), Kommentar zum Bucheffektengesetz (BEG) sowie zum HWpÜ und den relevanten Bestimmungen im OR und IPRG, Zürich/Basel/Genf 2013.

ECKERT MARTIN, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, S. 245–249.

– Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, S. 265–274.

ESSEBIER JANA/WYSS DOMINIC A., Von der Blockchain zu Smart Contracts, Jusletter vom 24. April 2017.

GLESS SABINE/KUGLER PETER/STAGNO DARIO, Was ist Geld? Und warum schützt man es?, recht 2015, S. 82–97.

GOBAT SÉBASTIEN, Les monnaies virtuelles à l'épreuve de la LP, AJP 2016, S. 1095–1105.

---

73 Vgl. zu einer Anpassung des Insolvenzrechts auch MAURENBRECHER/MEIER, Insolvenzrechtlicher Schutz, Rz 35 f.; WEBER, Blockchain, Rz 54.

74 Nach PILLER, Virtuelle Währungen, S. 1429, sollte Art. 713 ZGB in dem Sinn geändert werden, dass auch virtuelle Währungen Gegenstand des Fahrniseigentums sind. Vgl. hinsichtlich Daten im Allgemeinen WEBER/THOUVENIN, Dateneigentum, S. 49 ff., die sich gegen die Einführung eines Dateneigentums aussprechen und stattdessen punktuelle Ergänzungen des bestehenden Normenwerks befürworten.

75 EFD, Änderung des Bankengesetzes, S. 3 und 15.

GRAHAM-SIEGENTHALER BARBARA/FURRER ANDREAS, The Position of Blockchain Technology and Bitcoin in Swiss Law, Jusletter vom 8. Mai 2017.

HARI OLIVIER, La revendication et la distraction d'office d'actifs dans une procédure d'insolvabilité: application des principes aux monnaies cryptographiques, GesKR 2017, S. 453–468.

HAUSER-SPÜHLER GABRIELA/MEISSER LUZIUS, Eigenschaften der Kryptowährung Bitcoin, digma 2018, S. 6–12.

HÜRLIMANN DANIEL/ZECH HERBERT, Rechte an Daten, sui-generis 2016, S. 89–95.

KUHN HANS, Schweizerisches Kreditsicherungsrecht, Bern 2011.

JACQUEMART NICOLAS/MEYER STEPHAN D., Der Bitcoin-/Bitcoin-Cash-Hardfork, Die auftragsrechtliche Ablieferungspflicht bei Kryptowährungs-Dienstleistungen im Lichte der bundesgerichtlichen Rechtsprechung, GesKR 2017, S. 469–485.

LINDER THOMAS/MEYER STEPHAN D., Die steuerliche Behandlung von Bitcoin und anderen Kryptowährungen, ZStP 2017, S. 191–210.

MAURENBRECHER BENEDIKT/MEIER URS, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, Jusletter vom 4. Dezember 2017.

MEIER-HAYOZ ARTHUR, Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Sachenrecht, 1. Abteilung: Das Eigentum, 1. Teilband: Systematischer Teil und Allgemeine Bestimmungen, Artikel 641–654 ZGB, 5. Aufl., Bern 1981.

MEISSER LUZIUS, Kryptowährungen: Geschichte, Funktionsweise, Potenzial, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich/Basel/Genf 2015 (ZIK Band 61), S. 73–92.

MEYER STEPHAN D./SCHUPPLI BENEDIKT, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 2017, S. 204–224.

MIGNON VINCENT, Le « [B]itcoin », un nouveau défi pour le juriste suisse?, Jusletter vom 4. Mai 2015.

PILLER FRANÇOIS, Virtuelle Währungen – Reale Rechtsprobleme?, AJP 2017, S. 1426–1438.

REY HEINZ, Die Grundlagen des Sachenrechts und das Eigentum, Grundriss des schweizerischen Sachenrechts, Band I, 3. Aufl., Bern 2007.

ROTH GÜNTER H., Zur Zukunft des Wertpapierrechts, BJM 2011, S. 169–197.

SCHMID JÖRG/HÜRLIMANN-KAUP BETTINA, Sachenrecht, 5. Aufl., Zürich/Basel/Genf 2017.

SCHÖNKNECHT FLORIAN, Der Einlagebegriff nach Bankengesetz, GesKR 2016, S. 300–319.

SIXT ELFRIEDE, Bitcoins und andere dezentrale Transaktionssysteme, Blockchains als Basis einer Kryptoökonomie, Wiesbaden 2017.

STARK EMIL W./LINDENMANN BARBARA, Berner Kommentar, Schweizerisches Zivilgesetzbuch, Der Besitz, Art. 919–941 ZGB, 4. Aufl., Bern 2016.

STEINAUER PAUL-HENRI, Les droits réels, Band I, 5. Aufl., Bern 2012.

– Les droits réels, Band II, 4. Aufl., Bern 2012.

WEBER ROLF H., Blockchain als rechtliche Herausforderung, Jusletter IT vom 18. Mai 2017.

WEBER ROLF H./THOUVENIN FLORENT, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018 I, S. 43–74.

WIEGAND WOLFGANG, Vorbemerkungen zu Art. 641 ff. ZGB, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB, Art. 1–61 SchlT ZGB, 5. Aufl., Basel 2015.

ZOBL DIETER/GERICKE DIETER, Systematischer Teil des BEG, in: Zobl Dieter/Hess Martin/Schott Ansgar (Hrsg.), Kommentar zum Bucheffektengesetz (BEG) sowie zum HWpÜ und den relevanten Bestimmungen im OR und IPRG, Zürich/Basel/Genf 2013.

Materialien

Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, abrufbar unter: <www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>.

Botschaft des Bunderates zum Bucheffektengesetz sowie zum Haager Wertpapierübereinkommen vom 15. November 2006, BBl 2006, S. 9315–9420.

EFD, Änderung des Bankengesetzes und der Bankenverordnung (FinTech), Erläuternder Bericht zur Vernehmlassungsvorlage vom 1. Februar 2017.

FINMA, Bericht vom 1. August 2017: Wie sich Anleger gegen unerlaubt tätige Finanzmarktanbieter schützen können (abrufbar unter: <www.finma.ch>).

Unautorisierte Zahlungen mit virtuellen Währungen?

Martin Hess/Stephanie Lienhard, Zürich*

Inhaltsverzeichnis

* Dr. iur. Martin Hess, Rechtsanwalt, Partner bei Wenger & Vieli. MLaw Stephanie Lienhard, Rechtsanwältin.

I. Einleitung

Ende der 1. Maiwoche 2018 gab es gemäss Coinmarketcap[1] 1'614 virtuelle Währungen. Deren Marktkapitalisierung betrug zu diesem Zeitpunkt USD 457'141'660'679.[2]

Bitcoin (BTC) – die erste und bekannteste virtuelle Währung – war ursprünglich als Zahlungsmittel geschaffen worden.[3] In der Praxis sieht die Nutzung als Zahlungsmittel heute folgendermassen aus:

– Die Stadt Zug entschied im Mai 2016 als erste staatliche Institution weltweit, Bitcoin in begrenztem Umfang (bis CHF 200) als Zahlungsmittel zu akzeptieren.[4] Bei der Einwohnerkontrolle der Stadt Zug wurden von Mai 2016 bis Februar 2018 rund 50 Transaktionen mit Bitcoin beglichen. Das Zuger Handelsregisteramt akzeptiert seit November 2017, dass Dienstleistungen mit Bitcoin und Ether bezahlt werden können.[5] Bis Februar 2018 gab es nur drei Zahlungen in Höhe von gesamthaft 1'890 Franken, die beim Handelsregisteramt mit Bitcoin und Ether beglichen wurden. Zudem akzeptiert das Amt, dass bei der Gründung von Aktiengesellschaften und GmbH das Kapital mit Kryptowährungen liberiert werden kann. Kryptowährungen gelten ebenso als Sacheinlage wie beispielsweise Autos oder Mobiliar.[6]

---

1 Coinmarketcap ist ein Dienstleister, der alle gehandelten virtuellen Währungen auflistet: <https://coinmarketcap.com/>.

2 Vgl. <https://coinmarketcap.com/de/all/views/all/>.

3 NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System.

4 <http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/newsarchiv/?action=showinfo&info_id=351680>.

5 <https://www.zg.ch/behoerden/volkswirtschaftsdirektion/handelsregisteramt/aktuell/handelsregisteramt-zug-akzeptiert-kryptowaehrungen-bitcoin-und-ether-als-zahlungsmittel>.

6 Neue Zürcher Zeitung (NZZ) vom 10. Februar 2018, «Die Bitcoinblase platzt – im Zuger Crypto Valley wachsen die Bedenken», <https://www.nzz.ch/schweiz/die-bitcoin-blase-platzt-im-zuger-crypto-valley-wachsen-die-bedenken-ld.1354992>.

– Pro Tag werden in Deutschland 70 Mio. Zahlungen getätigt, weltweit mit Bitcoin nur ca. 300'000.[7]

Folglich finden virtuelle Währungen wie Bitcoin und Ether in der Regel keine Verwendung als Zahlungsmittel, sondern sind Anlage- und Spekulationsinstrumente. Demzufolge sind Transaktionen in virtuellen Währungen häufig, Zahlungen nicht.

II. Geld und Währungen

1. Grundlagen der geltenden Geld- und Währungsordnung

Die Währungshoheit, d.h. die Kompetenz, Regeln betreffend das Geld- und Währungswesen zu erlassen, liegt in der Regel in staatlichen Händen, in der Schweiz beim Bund.[8]

Der Begriff des «Geldes» ist unscharf. Gemäss der allgemeinen Geldtheorie hat Geld drei Funktionen. Geld ist:

- ein Zahlungsmittel,
- eine Recheneinheit (Vergleichsmassstab), und
- ein Wertaufbewahrungsmittel (Sparen).[9]

«Geld» in seiner konkreten Funktion als Zahlungsmittel wird in Art. 2 des Bundesgesetzes über die Währung und die Zahlungsmittel[10] definiert als die vom Bund ausgegebenen Münzen, die von der Schweizerischen Nationalbank (SNB) ausgegebenen Banknoten und die auf Franken lautenden Sichtguthaben bei der SNB.

Eine weitere Art von «Geld» ist das Buchgeld der Geschäftsbanken. Die Geschäftsbanken halten Geld auf Bankkonten (sog. Buchgeld). Buchgeld entsteht durch Einzahlung von Bargeld auf Bankkonti oder mittels Kreditvergabe, indem die Banken den Kunden die als Kredit gewährten Beträge auf deren Konto gutschreiben. Buchgeld ist immer eine Forderung gegen-

---

7 Neue Zürcher Zeitung (NZZ) vom 15. Februar 2018, «Kryptowährungen: ‹Nicht auf jede Neuerung muss ein Verbot folgen›», <https://www.nzz.ch/wirtschaft/nicht-auf-jede-neuerung-muss-ein-verbot-folgen-ld.1357501>.

8 Art. 99 Abs. 1 BV (SR 101).

9 Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 7; CARSTENS, Money, S. 2 ff.

10 WZG (SR 941.10).

über dem kontoführenden Finanzinstitut und damit von dessen Bonität abhängig.[11]

Währung bezeichnet das hoheitlich geordnete Geldwesen eines Staates einschliesslich aller Regelungen zur Sicherung der Geldwertstabilität (Währungsverfassung), die Denominierung, die befreiende Wirkung bei Verwendung als Zahlungsmittel und die allfällige Annahmepflicht (Zwangskurs).[12]

Eine Währung setzt sich nur durch, wenn sie Vertrauen geniesst:

> *«History shows that money as a convention needs to have a basis of trust, supported by some form of institutional arrangement.»*[13]

2. Merkmale von virtuellen Währungen

a) Rechtliche Einordnung

Virtuelle Währungen sind digitale Darstellungen von im Internet handelbaren Werten, die die Funktion von Geld übernehmen, aber nicht als gesetzliche Zahlungsmittel akzeptiert sind.[14]

Virtuelle Währungen vermitteln keinen Anspruch gegen einen Herausgeber.[15]

Die Volatilität[16] der virtuellen Währungen verunmöglicht den Gebrauch als Wertmassstab. Der Wert von Bitcoin und Ether wird nach wie vor in gesetzlichen Zahlungsmitteln angegeben. Die Volatilität gefährdet auch die Verwendung als Wertaufbewahrungsmittel.[17]

Virtuelle Währungen sind nicht gesetzliche Zahlungsmittel i.S. von Verfassung und Gesetz (Art. 99 BV, Art. 1 und 2 WZG und Art. 84 OR).[18]

Das Entwickeln und Anbieten privater (d.h. nicht gesetzlicher) Zahlungsmittel verstösst nicht gegen das Schweizer Währungsrecht.[19] Zivilrecht-

---

11 GIOVANOLI, FS KLEINER, S. 87 ff.

12 ZELLWEGER-GUTKNECHT, Digitale Landeswährung, S. 5.

13 CARSTENS, Money, S. 3.

14 HESS/SPIELMANN, Cryptocurrencies, S. 175 m.w.H.

15 FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, S. 2.

16 HESS/SPIELMANN, Cryptocurrencies, S. 174 f.

17 CARSTENS, Money, S. 9 f.

18 GRÜNEWALD, Virtuelle Währungen, S. 93 ff. Siehe dazu auch den Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 5 ff.

19 GRÜNEWALD, Virtuelle Währungen, S. 98 Fn. 21.

lich sind private Zahlungsmittel – u.a. Buchgeld, WIR-Geld, virtuelle Währungen – daher nicht verboten, sofern die Beteiligten in deren Verwendung als Zahlungsmittel einwilligen. Anwendbar auf diese Fälle sind die Bestimmungen des Vertragsrechts, insbesondere des Obligationenrechts.[20]

Virtuelle Währungen sind daher Vermögenswerte und Zahlungsmittel, sofern Letzteres zwischen den Parteien vereinbart worden ist.[21]

b) Die verschiedenen Arten des Vertrauens in Währungen und Zahlungsmittel[22]

Ein horizontales Vertrauensverhältnis kann zwischen Individuen bestehen, beispielsweise bei einem Tauschgeschäft oder beim Wechsel, der letztlich den persönlichen Kredit des Ausstellers verbrieft.

Ein vertikales Vertrauensverhältnis besteht zwischen Finanzinstituten und deren Kunden. Das Vertrauen in die Finanzinstitute wird durch die Rechtsordnung gestärkt.

In der digitalen Ökonomie gilt das verteilte Vertrauen (*distributed trust/distributed consensus*).[23] Dieses stützt sich auf Algorithmen, digitale Protokolle sowie Netzwerke voller Daten.

III. Technische Grundlagen

1. Blockchain Technologie als Basis virtueller Währungen

Die meisten virtuellen Währungen basieren grundsätzlich auf der sog. Blockchain Technologie.[24] Dabei handelt es sich um ein dezentrales Netz-

---

20 Bericht des Bundesrates zu virtuellen Währungen vom 25. Juni 2014, S. 7, 10; HESS/KALBERMATTER/WEISS, SK FinfraG, Art. 81 N 22 Fn. 46.

21 HESS/SPIELMANN, Cryptocurrencies, S. 175 f.

22 Neue Zürcher Zeitung (NZZ) vom 3. Februar 2018, S. 29, «Wie vertraut man einem Algorithmus?».

23 SZABO, Trusted Third Parties, Abschnitte «TTP Minimizing Protocols» und «Conclusion». Zum Distributed Consensus siehe unten Abschnitt III. 1.

24 Ein gegenteiliges Beispiel ist IOTA: <https://iotasupport.com/whatisiota.shtml>. Das zugrundeliegende Protokoll orientiert sich zwar ebenfalls an der Distributed Ledger Technologie, die Transaktionen werden jedoch parallel über einen sog. Tangle – ein directed acyclic graph (DAG) – bearbeitet und der Sender einer Transaktion ist gleichzeitig für die Verifizierung von zwei vorhergehenden Transaktionen zuständig, was das

werk, welches in der einen oder anderen Form Transaktionen verifiziert, in Blöcken zusammenfasst und in der Folge im jeweiligen Block registriert. Bei der Bitcoin Blockchain verifizieren sog. Full Blockchain Nodes[25] unabhängig voneinander und anhand einer langen Liste von Kriterien die einzelnen Transaktionen, bevor sie diese ans Netzwerk weiterleiten.[26] In der Folge werden diese verifizierten Transaktionen durch sog. Miner in einen neuen Block zusammengefasst, welcher erst nach erfolgreicher Berechnung eines komplizierten Algorithmus den sog. Proof of Work und damit Gültigkeit erlangt.[27] Schliesslich verifizieren die Nodes den neuen Block erneut unabhängig voneinander und anhand einer langen Liste von Kriterien, bevor sie ihn im Netzwerk verteilen und in ihre eigene Blockchain-Kopie aufnehmen.[28]

Der Prozess, durch welchen sich das dezentrale Netzwerk von Teilnehmern auf einen einzigen gültigen Status der Blockchain einigt, unterscheidet sich teilweise zwischen den verschiedenen virtuellen Währungen. Die auf Bitcoin basierenden Währungen wie beispielsweise Litecoin[29] oder das Monero zugrunde liegende CryptoNote-Protokoll[30] sowie zurzeit auch noch Ethereum stützen sich auf den vorgängig umschriebenen Proof of Work. Daneben gibt es zahlreiche Varianten von Konsens-Algorithmen, welche auf unterschiedlich ausgestalteten Proposal- und Voting-Funktionen der Nodes basieren. Wenn das Gewicht eines Proposals oder eines Votes davon abhängig ist, wie viele Einheiten der jeweilige Node von der blockchain-eigenen virtuellen Währung besitzt bzw. als Depot hinterlegt, spricht man vom sog. Proof of Stake.[31] Des Weiteren gibt es auch einen sog. Proof of Importance,

---

Senden erst ermöglicht. Für das technische Whitepaper siehe: <http://iotatoken.com/IOTA_Whitepaper.pdf>.

25 Diese Nodes speichern jeweils die gesamte Blockchain seit der ersten Transaktion im ersten Block; vgl. hierzu ANTONOPOULOS, Mastering Bitcoin, S. 145 f.

26 ANTONOPOULOS, Mastering Bitcoin, S. 177 f.

27 ANTONOPOULOS, Mastering Bitcoin, S. 179 f., 188 f.

28 ANTONOPOULOS, Mastering Bitcoin, S. 197 ff.

29 <https://litecoin.org>.

30 Siehe dazu <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>.

31 Für einen anschaulichen Vergleich zwischen Proof of Work und Proof of Stake siehe: ROSIC, Proof of Work vs Proof of Stake; für die bei Ethereum geplante Implementierung des Proof of Stake basierten Casper Systems: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ> sowie <https://github.com/ethereum/research/blob/master/p

bei welchem die Transaktionshäufigkeit sowie das Transaktionsvolumen für die Schaffung eines Blocks massgebend ist.[32]

Was aber wohl die meisten virtuellen Währungen grundsätzlich gemeinsam haben, ist die Datenstruktur eines Blocks. So besteht ein Block u.a. aus der Liste aller in ihm zusammengefassten Transaktionen[33] sowie dem Hash[34] des vorhergehenden Blockes. Dieser Hash wiederum beinhaltet die Datenstruktur des gesamten letzten Blockes und jeder neue Block wird dadurch mit dem vorherigen insoweit verbunden, als der neue Datensatz immer auch den Hash und damit die Transaktionsdaten des vorhergehenden beinhaltet. Eine Änderung in Block x würde also auch alle darauffolgenden Blöcke verändern.[35]

2. Kryptographisch ausgestaltete Transaktionen

Grundlage für alle Transaktionen über ein Blockchain Netzwerk sind kryptographische Schlüssel und die entsprechenden Funktionen, wobei die Ausgestaltung im Detail variieren kann. Basis bildet in der Regel ein Schlüsselpaar, bestehend aus einem Private und einem Public Key. Der Private Key besteht aus einer beliebig festgelegten Zahlenreihenfolge. Der Public Key errechnet sich mittels einer mathematischen Formel – genauer gesagt einer elliptischen Kurve – aus dem Private Key. Ähnliches geschieht mit der Bit-

apers/casper-basics/casper_basics.pdf>; für ein weiteres Beispiel: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#consensus-algorithm-bft-dpos>, <https://cardanodocs.com/cardano/proof-of-stake>.

32 <https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf>.

33 Diese werden oftmals mittels eines sog. Merkle Trees in einem kleineren Datenformat zusammengefasst; für Bitcoin siehe ANTONOPOULOS, Mastering Bitcoin, S. 160 f., 164 ff.; DECKER/WATTENHOFER, Information Propagation, S. 2 f.

34 Ein Hash Algorithmus ist eine Einwegfunktion, die eine beliebig grosse Eingabemenge bzw. Zeichenfolge in einem digitalen Fingerabdruck in Form einer kleineren, fixen Zielmenge bzw. Zeichenfolge abbildet; ANTONOPOULOS, Mastering Bitcoin, S. 71, 188. Siehe auch die Einträge bei WIKIPEDIA: <https://de.wikipedia.org/wiki/Hashfunktion>; <https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion>.

35 ANTONOPOULOS, Mastering Bitcoin, S. 159 ff.; <https://bitcoin.org/en/developer-guide#block-chain>.

coin-Adresse, welche – durch eine Hash[36] Funktion – grundsätzlich aus dem Public Key generiert wird.[37]

Die Bitcoin-Adresse ist derjenige Datensatz, welcher als Empfänger für eine Transaktion kommuniziert werden kann, während mit dem Private Key eingehende oder ausgehende Transaktionen verifiziert werden.[38] Die mathematischen Formeln bewirken, dass anhand des Private Keys der Public Key generiert werden kann und darauf basierend die Bitcoin-Adresse; umgekehrt ist dies allerdings nicht möglich. Dasselbe geschieht mit sog. Signaturen, welche vom Private Key abgeleitet werden.[39]

Die vom Private Key abgeleitete Signatur wird für jede Transaktion wieder neu generiert, kann aufgrund der mathematischen Abhängigkeit zwischen Private und Public Key immer mit dem korrespondierenden Public Key in Verbindung gebracht werden und lässt gleichzeitig aber keinen Rückschluss auf den Private Key zu. Die Signatur ermöglicht somit, die Verfügungsgewalt an einzelnen Werten aufzuzeigen, ohne den Private Key preiszugeben.[40]

IV. Unautorisierte Zahlungen

1. Zentralisiert

a) Autorisierung, Authentisierung und Authentifizierung

Finanzinstitute halten die Vermögenswerte der Kunden auf Konti oder in Depots. Der Kunde kann darüber verfügen, wenn er sich als Berechtigter ausweist und eine entsprechende Weisung erteilt. Dieser Prozess setzt sich zusammen aus «Autorisierung», «Authentisierung» und «Authentifizierung».[41]

Die Authentisierung stellt den Nachweis einer Person dar, dass sie tatsächlich diejenige Person ist, die sie vorgibt zu sein.

---

36 Vgl. Fn. 34.

37 Vorliegend dient Bitcoin als Anschauungsbeispiel. Zum Ganzen daher: ANTONOPOULOS, Mastering Bitcoin, S. 61 ff., 65, 70 f.

38 ANTONOPOULOS, Mastering Bitcoin, S. 61, 63, 70.

39 ANTONOPOULOS, Mastering Bitcoin, S. 63 f., 65 ff., 70 ff.

40 ANTONOPOULOS, Mastering Bitcoin, S. 62.

41 AGNIESZKA CZERNIK, Authentisierung, Authentifizierung und Autorisierung.

Die Authentifizierung stellt eine Prüfung der behaupteten Authentisierung dar. In den Worten der PSD 2 ist es «*das Verfahren, mit dessen Hilfe ein Finanzinstitut die Identität eines Zahlungsdienstnutzers oder die Verwendung eines Zahlungsinstruments überprüfen kann*».[42]

Die Autorisierung ist die Einräumung von speziellen Rechten. War die Identifizierung einer Person erfolgreich, heisst es noch nicht automatisch, dass diese Person bereitgestellte Dienste und Leistungen nutzen darf. Darüber entscheidet die Autorisierung. Beispielsweise gilt ein Zahlungsvorgang als autorisiert, wenn der Zahler diesem zugestimmt hat (Art. 64 PSD 2).

In der zentralisierten Struktur mit einzeln kontoführenden Finanzinstituten erfolgen Autorisierung, Authentisierung und Authentifizierung jeweils im bilateralen Verhältnis zwischen Finanzinstitut und Kunde. Die entsprechenden Regeln sind in Verträgen und allgemeinen Geschäftsbedingungen festgehalten. Bei fehlerhaften Vorgängen betreffend Autorisierung, Authentisierung und Authentifizierung regeln Gesetz[43] oder Gerichtspraxis[44] die Rechtsfolgen, insbesondere die Haftung.

b) Widerruf

Im geltenden Schweizer Recht ist der Widerruf geregelt in Art. 470 Abs. 2bis OR für die bargeldlose Überweisung[45] und in Art. 15 Abs. 3 BEG für Transaktionen in Bucheffekten[46]:

- Nach Art. 470 Abs. 1 OR kann eine Anweisung grundsätzlich jederzeit widerrufen werden, es sei denn, der Angewiesene habe dem Anweisungsempfänger Annahme erklärt (Art. 470 Abs. 2 OR). Art. 470 Abs. 2bis OR lässt für Anweisungen im bargeldlosen Zahlungsverkehr Unwiderruflichkeit mit der Belastung des Kontos des Zahlers durch den angewiesenen Finanzintermediär eintreten. Vorbehalten bleiben abweichende Regeln von Zahlungssystemen.

---

42 Art. 4 Ziff. 29 PSD 2.

43 Zu den Art. 73 und 74 PSD 2 siehe EMMENEGGER, Eckpunkte, S. 47 ff.; zu den entsprechenden Bestimmungen in der PSD 1 siehe HESS, Euro-Zahlungen, S. 88 ff.

44 HESS, Euro-Zahlungen, S. 90 ff.

45 HESS, Euro-Zahlungen, S. 76 ff.; HESS/STÖCKLI, Bucheffektengesetz, S. 109 f.

46 HESS/ZBINDEN, BEG-Kommentar, N 31 ff. zu Art. 15 BEG; HESS/STÖCKLI, Bucheffektengesetz, S. 109.

- Nach dem Wortlaut von Art. 15 Abs. 3 BEG ist ein Widerruf immer dann nicht mehr möglich, sobald das Effektenkonto des Kontoinhabers belastet wurde.

Sowohl im bargeldlosen Zahlungsverkehr wie bei der Effektenabwicklung erfolgt der Widerruf gegenüber dem kontoführenden Finanzinstitut. Die Regeln betreffend Widerruf sind auf die heutige zentralisierte Finanzmarktinfrastruktur zugeschnitten, welche auf vertikalem Vertrauen basiert. Die Finanzinstitute führen zentral Konti und sind somit Ansprech- und Vertragspartner des Kunden.

Es besteht vertikales Vertrauen. Mit Blick auf das verteilte Vertrauen bei virtuellen Währungen stellt sich die Frage: An wen soll man sich bei einem Widerruf halten?

c) Stornierung

In der zentralisierten Struktur der Finanzwelt ist die Stornierung einer infolge fehlender oder unwirksamer Weisung/Anweisung zu Unrecht erfolgten Transaktion durch das kontoführende Finanzinstitut möglich. Im Effektenbereich bilden Art. 27/28 BEG[47] die Rechtsgrundlage, im Zahlungsverkehr ist die Stornierungsmöglichkeit zumeist stillschweigender Vertragsinhalt.[48]

Auch bezüglich der Stornierung stellt sich für ein dezentrales Netzwerk unweigerlich die Frage nach deren Praktikabilität: Wer ist autorisiert und in der Lage, eine Transaktion rückgängig zu machen, insbesondere angesichts der erschwerten Abänderlichkeit der auf der Blockchain registrierten Daten?[49]

2. Dezentral

a) Verifizierung

Wie ausgeführt wurde, werden Transaktionen in virtuellen Währungen regelmässig mittels einer vom Private Key abgeleiteten Signatur verifiziert. Der Inhaber des Private Keys kann somit eine Transaktion auslösen. Erfolgt diese Verifizierung, wird die Anzahl der von der Transaktion betroffenen

47 HESS/STÖCKLI, Bucheffektengesetz, S. 110 ff.; WEBER, BEG Kommentar zur Art. 27 und 28 BEG, passim.

48 BUIS, Stornorecht, S. 126, 128.

49 Abschnitt IV.2.c nachstehend.

virtuellen Währungen der mit dem Private Key verbundenen Bitcoin-Adresse zugewiesen. Die Transaktion ist im Grundsatz abgeschlossen, sobald die Mehrheit der am Netzwerk Beteiligten diese Zuweisung akzeptiert und in die aktuelle Version der Blockchain aufnimmt.

Wird die Transaktion von den Netzwerkteilnehmern nicht akzeptiert, gelangt sie nicht in einen Block und/oder wird sie nicht von der Mehrheit der Nodes in die Blockchain aufgenommen, gilt die entsprechende Transaktion als nicht vorhanden. Damit würde zwar eine verifizierte Zahlung vorliegen, sie hätte für das Netzwerk aber keinerlei Relevanz.

Wenn eine Transaktion mittels eines fremden, allenfalls gestohlenen Private Keys signiert wird, ist die Ausgangslage vorderhand ähnlich wie bei einer traditionellen Bankzahlung: Der die Transaktion Auslösende gibt sich mittels des von der Bank bzw. dem Netzwerk anerkannten Verifizierungsverfahrens als Berechtigter aus und wird auch als solcher anerkannt. Denn das Netzwerk verifiziert eine Transaktion nur anhand der vom Private Key abgeleiteten, korrekten Signatur. Wird eine Transaktion auf Basis eines kryptographisch richtigen Private Keys signiert, werden die Mehrzahl der Nodes die Transaktion verifizieren und im Netzwerk verteilen. Somit kann ein Verlust des Verifizierungsmerkmals, also des Private Keys, bei genauer Betrachtung auch bei Transaktionen in virtuellen Währungen zu einer unautorisierten Zahlung führen. Wie zu zeigen sein wird, unterscheiden sich allerdings die Folgen einer unautorisierten Zahlung in diesem Bereich diametral vom Konzept, welches dem traditionellen Zahlungsverkehr zugrunde liegt.[50]

b) Cold Storage und Co.

Damit sich niemand eines fremden Private Keys bedient, gibt es mittlerweile zahlreiche Varianten, einen Verlust mit grösstmöglicher Sicherheit zu verhindern.

Wie bereits ausgeführt, können virtuelle Währungen an sich nicht gehalten oder verwahrt werden, da es sich hierbei um öffentlich zugängliche Datenstränge handelt. Will man seinen Bestand an virtuellen Währungen sicher verwahren, so ist hierfür der Private Key entsprechend sicher aufzubewahren.

Während eine starke Verschlüsselung und ein Backup der Wallet bzw. der darin abgespeicherten Private Keys stark an andere passwortgeschützte

[50] Abschnitt IV.2.c/d nachstehend.

Konten erinnert, scheint das sog. Cold Storage trotz Digitalisierung das Rad der Zeit wieder um Jahrzehnte zurückzudrehen. Bei der Cold Storage werden die Private Keys offline, also ohne Zugang zum Internet verwahrt. Dies soll insbesondere Hackerangriffen vorbeugen. Noch mehr Sicherheit wird erreicht, wenn man bereits bei der Schaffung des Private Keys auf eine Verbindung zum Internet verzichtet. [51]

Für den täglichen Gebrauch ist diese Art der Verwahrung jedoch mühsam, da Transaktionen nur über eine Internetverbindung möglich sind. Dies führt dazu, dass die Guthaben in virtuellen Währungen oft aufgeteilt werden in einen grossen Betrag, welcher offline als eine Art Sparguthaben lagert und in einen kleineren Betrag für den täglichen Gebrauch mittels einer sog. Hot Wallet, welche mit dem Internet verbunden ist.[52]

Zahlreiche Handelsplattformen (sog. Cryptocurrency Exchanges) geben an, dass sie die Mehrheit der Kundenvermögen offline verwahren.[53] Allerdings gibt es immer wieder Berichte von erfolgreichen Hackerangriffen auf Hot Wallets und die Verwahrung von Kundenvermögen in Cold Wallets scheint sich noch nicht überall durchgesetzt zu haben.[54]

Cold Storage kann beinahe klassisch über ein sog. Paper Wallet erfolgen. Dabei sind der Private und Public Key auf einem Stück Papier aufgedruckt und oftmals noch mit einem QR-Code versehen, damit ein Einlesen mittels eines digitalen Gerätes möglich wäre.[55] Da auf dem Papier aber sämtliche relevanten Daten ersichtlich sind, muss das Papier entsprechend sicher auf-

---

51 <https://en.bitcoin.it/wiki/Cold_storage>; BAJPAJ, What Is Cold Storage For Bitcoin; <https://www.bitcoin.com/guides/setting-up-your-own-cold-storage-bitcoin-wallet>; ANTONOPOULOS, Mastering Bitcoin, S. 104 f.

52 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin.

53 So z.B. Kraken <https://www.kraken.com/en-us/security/practices>; Bitfinex <https://www.bitfinex.com/legal/security_policy>; Coinbase <https://www.coinbase.com/security>; Bittrex: <https://support.bittrex.com/hc/en-us/articles/115003684411>.

54 Für den Hack der japanischen Cryptocurrency Exchange Coincheck siehe ALPEYEV/NAKAMURA, How to Launder $500 Million in Digital Currency; WELTER, Hackerangriff trifft japanische Krypto-Börse; im Fall BitGrail besteht zumindest das Risiko, dass die Verwahrung in einer Hot Wallet den Hack ermöglicht hatte: YOUNG, BitGrail Vs. Nano.

55 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin; ANTONOPOULOS, Mastering Bitcoin, S. 104 ff. Für mögliche Tools zur Generierung der Keys siehe <https://tools.bitcoin.com/paper-wallet>; <https://walletgenerator.net>.

bewahrt und vor Blicken und Zugang Dritter geschützt werden.[56] Um die Sicherheit zu erhöhen, ist es allerdings auch möglich, dass auf dem Paper Wallet ein verschlüsselter Private Key angezeigt wird, welcher nur in Kombination mit einem zusätzlichen Passwort gültig ist.[57]

Des Weiteren kann der Private Key auch auf einem USB Stick gespeichert werden und dieser Stick dann sicher verwahrt werden, z.B. in einem Tresor. Ähnlich funktionieren sog. Hardware Wallets, welche meist als UBS Stick mit mehr oder weniger Zusatzfunktionen ausgestaltet sind und – sobald mit dem Internet verbunden – auch Transaktionen ermöglichen.[58]

Eine weitere Variante ist schliesslich ein sog. Sound Wallet. Der Private Key wird hier in verschlüsselter Form von einer Bild- in eine Audio-Datei umgewandelt und auf einer CD oder sogar Vinyl Platte verewigt. Der Private Key kann sodann nur mittels eines Spektrometers gelesen werden, wobei die Audio-Datei hierfür wieder in eine Bilddatei umgewandelt wird.[59]

All diese Möglichkeiten von Cold Storage haben gemeinsam, dass sie in traditioneller Weise sicher verwahrt werden müssen (z.B. Tresor, Schliessfach). Dies gipfelt sogar in Angeboten für Verwahrung im Untergrund über mehrere Kontinente verteilt.[60]

c) Stark erschwerte Abänderlichkeit

Wie bereits angetönt, liegt das eigentliche Problem einer unautorisierten Zahlung im Bereich der virtuellen Währungen an faktischen Gegebenheiten. Es wurde dargelegt, dass die Verifizierung von Transaktionen zum einen dezentral erfolgt und zum anderen die einzelnen Transaktionen in Blöcken, welche miteinander verbunden sind, zusammengefasst werden.

Tritt nun der Fall ein, dass jemand mit einem fremden Private Key eine unautorisierte Transaktion ins Netzwerk schickt, wird diese mutmasslich von allen oder zumindest der Mehrheit der Nodes als korrekt verifiziert und im Netzwerk verteilt werden. In der Folge wird die Transaktion im Rahmen des anwendbaren Konsens-Algorithmus in einen Block integriert und dieser nach Verifikation wieder im Netzwerk verteilt. Die unautorisierte Zahlung

---

56 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin; ANTONOPOULOS, Mastering Bitcoin, S. 104 ff.; <https://walletgenerator.net>.

57 ANTONOPOULOS, Mastering Bitcoin, S. 105 f.

58 ROSIC, Paper Wallet Guide; BAJPAJ, What Is Cold Storage For Bitcoin.

59 ULM, Listen to your Bitcoins with Sound Wallet; THOMA, Sound Wallet.

60 Vgl. hierzu <https://xapo.com/vault>.

wird also mehrfach von einer unzählbar grossen Teilnehmerzahl bearbeitet, ohne dass es eine zentrale Anlaufstelle geben würde, bei welcher eine Rückabwicklung begehrt werden könnte.

Als wäre dies nicht bereits genug, wird das Ganze durch die Aneinanderreihung der einzelnen Blöcke noch zusätzlich erschwert. Der Block x, in welchen die unautorisierte Transaktion aufgenommen wurde, wird sowohl durch die Daten der Transaktion wie auch durch die Daten bzw. den Hash des vorherigen Blockes x-1 bestimmt. Zusätzlich wird jeder darauffolgende Block x+n auch die Daten des Blockes x und damit der unautorisierten Transaktion enthalten. Damit wäre eine Rückabwicklung mit einem so grossen technischen, aber auch energetischen und damit finanziellen Aufwand verbunden, dass dies für einen normalen Teilnehmer schlicht nicht möglich ist. Sollte also der Widerruf oder die Stornierung bzw. allgemein die Rückabwicklung einer Transaktion nicht bereits aufgrund der dezentralen Struktur der Blockchain ausgeschlossen sein, so würde sie spätestens aufgrund des zu grossen Aufwandes unrealistisch.

d) Fork als Spezialfall

Der Grundsatz, dass Transaktionen aufgrund der vorgängig umschriebenen Funktionsweise nachträglich nicht mehr geändert werden können, erfährt im Zusammenhang mit sog. Forks einen Vorbehalt.

Grundsätzlich sind gewisse Gabelungen oder Neudeutsch Forks der Blockchain Technologie immanent. Sie erfolgen regelmässig dann, wenn zwei gültige Blöcke gleichzeitig innert eines kurzen Zeitabstandes geschaffen werden und zu einer Abweichung der Ansichten der verschiedenen Netzwerkteilnehmer betreffend die korrekte Transaktionshistorie führen.[61] Normalerweise ist dies ein vorübergehender Zustand, da sich bald die längste Kette durchsetzt und sich dann wieder alle Nodes auf eine richtige Kette einigen.[62]

---

61 ANTONOPOULOS, Mastering Bitcoin, S. 200 f.; <https://bitcoin.org/en/developer-guide#block-chain>; DECKER/WATTENHOFER, Information Propagation, S. 3 und 6; CASTOR, A Short Guide to Bitcoin Forks.

62 ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 04:30; ANTONOPOULOS, Mastering Bitcoin, S. 200; DECKER/WATTENHOFER, Information Propagation, S. 3; CASTOR, A Short Guide to Bitcoin Forks.

Ein Fork kann jedoch auch bei der Weiterentwicklung der den jeweiligen virtuellen Währungen zugrundeliegenden Open Source Software erfolgen.[63] Wird eine neue Regel in den Code integriert, welche es auch denjenigen Nodes, welche das Update (noch) nicht implementiert haben, ermöglicht, Transaktionen zu verifizieren und zu akzeptieren, spricht man von einem sog. *Soft Fork*. Die Regeln für die Gültigkeit von Transaktionen werden mit der neuen Software Version strenger und diese ist abwärtskompatibel. Die Nodes mit der aktualisierten oder neuen Software lehnen Transaktionen, welche nach der alten Softwareversion gültig gewesen wären, ab. Dagegen können diejenigen Nodes, welche noch die alte Version nutzen, auch Transaktionen basierend auf dem neuen Standard bearbeiten und akzeptieren. Damit ist weiterhin eine Teilnahme der Nodes möglich, welche die neue Regel noch nicht implementiert haben. Zur Veranschaulichung diene hier die Verkleinerung der Blockgrösse von 1MB auf 500kB: Ein Node mit neuer Software weist jeden Block ab, der die Grösse von 500kB überschreitet, während der Node mit der ursprünglichen Software generell Blöcke bis 1MB und damit auch 500kB akzeptieren kann.[64]

Die vorgängig umschriebene Art eines Forks unterscheidet sich vom sog. *Hard Fork*. Hierbei erfolgt eine Code-Änderung, die dazu führt, dass Transaktionen, welche nach den neuen Regeln gültig sind, von den Nodes, welche das Update nicht implementieren, zurückgewiesen werden. Die Regeln für die Gültigkeit von Transaktionen werden lascher und es mangelt hier an der Kompatibilität der neuen Software mit der alten. Wird das Update folglich nicht von allen Nodes übernommen, kommt es zu einer Spaltung der Blockchain, in eine mit und in eine ohne das entsprechende Update.[65] Ein Beispiel für einen Hard Fork ist die Abspaltung der Bitcoin Cash Blockchain am 1.

---

63 <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; CASTOR, A Short Guide to Bitcoin Forks.

64 Vgl. zum Ganzen: ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 09:45; <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; <https://bitcoin.org/en/developer-guide#consensus-rule-changes>; CASTOR, A Short Guide to Bitcoin Forks; bitcoin*wiki*, Softforks, <https://en.bitcoin.it/wiki/Softfork>.

65 Vgl. zum Ganzen: ANTONOPOULOS, Forkology: A Study of Forks for Newbies, ab 09:45; <https://www.btc-echo.de/tutorial/der-fork-guide-was-ist-eine-fork-und-welche-arten-gibt-es-soft-fork-hard-fork-uasf-masf>; <https://www.investopedia.com/terms/h/hard-fork.asp>; <https://bitcoin.org/en/developer-guide#consensus-rule-changes>; CASTOR, A Short Guide to Bitcoin Forks.

August 2017: Die neue Blockgrösse von 8MB kann nur von Nodes/Minern akzeptiert werden, die das entsprechende Update durchgeführt haben. Mit einer älteren, auf Blöcke von 1MB ausgerichteten, Version der Software ist die Verarbeitung von 8MB-Blöcken nicht möglich.[66]

Durch Forks werden also Transaktionen neuen Regeln unterstellt, sodass ursprünglich gültige Transaktionen ungültig oder ursprünglich ungültige Transaktionen allenfalls sogar gültig werden.

Für eine Rückabwicklung im Fall einer unautorisierten Zahlung taugen diese Mechanismen allerdings nicht. Vielmehr sind sie mit zusätzlichen Risiken verbunden. Neben der generellen Unsicherheit während der Umstellung auf eine neue Software-Version, besteht im Falle von Hard Forks insbesondere das Problem von sog. Replay Attacks. Da die technologische Basis der gespaltenen Blockchain jeweils dieselbe ist,[67] besteht die Gefahr, dass eine Transaktion zweimal – sowohl in der ursprünglichen als auch in der abgespaltenen, neuen Blockchain – ausgeführt wird.[68]

V. Haftung

1. In der zentralisierten Welt

Das Schweizer Zivilrecht regelt die Haftung zwischen Vertragsparteien und bei unerlaubten Handlungen. Dabei setzt es voraus, dass der Schuldner (Art. 97 ff. OR) respektive der Ersatzpflichtige (Art. 41 OR) bekannt sind. Es gibt Rechtssubjekte, die man ins Recht fassen kann. Den meisten Dienstleistungen im Finanzbereich liegt üblicherweise ein Auftragsverhältnis zwischen dem Anbieter des Dienstes und dem Benutzer zu Grunde. Der Beauftragte bzw. der Anbieter einer Dienstleistung ist zur getreuen Geschäftsführung nach Art. 398 OR verpflichtet und untersteht somit der auftragsrechtlichen Sorgfalts- und Treuepflicht. Vom Beauftragten wird gefordert, alles zu tun, um die richtige Erfüllung der Hauptleistung und die Verwirklichung des Leistungserfolges zu sichern und dabei das Integritätsinteresse des

66 BERGMANN, Was passiert bei einem Hard Fork?; BERGMANN, Das kleine 1x1 zur Bitcoin Cash Fork.

67 So erhält der Nutzer bei einem Hard Fork grundsätzlich gleich viele Einheiten der neuen virtuellen Währung, wie er bereits von der alten besitzt, wobei die neuen Einheiten ursprünglich dem gleichen Schlüsselpaar zugeordnet sind.

68 HERTIG, Rise of Replay Attacks; SONG, Replay Attacks Explained.

Gläubigers zu beachten. Unsachgemässes, unsorgfältiges Verhalten wird deshalb grundsätzlich als Vertragsverletzung aufgefasst.[69]

Das Aufsichtsrecht[70] stipuliert Pflichten für regulierte Finanzinstitute, Banken, Effektenhändler etc., welche sowohl aufsichtsrechtlich relevant sind als auch zur Konkretisierung der zivilrechtlichen Sorgfaltspflicht dienen können. Als Beispiel kann das Rundschreiben der FINMA «Operationelle Risiken Banken» erwähnt werden, insbesondere dessen Anhang 3 «Umgang mit elektronischen Kundendaten».[71] Weitere Regeln inklusive Haftungsbestimmungen finden sich im Datenschutzrecht[72] sowie im Strafrecht.[73]

2. Haftungssubjekt in der dezentralen Welt?

Die dezentrale Welt zeichnet sich aus durch transnationale, mehrschichtige Gemeinschaften von Nutzern und Beitragserbringern (User, Miner etc.). Es gibt weder einen eindeutig bestimmbaren Ort, an dem anzuknüpfen wäre, noch eine eindeutig als Verursacher bestimmbare Person.

Gegen wen geht man vor bei dezentral geschaffenen Applikationen? Wer ist beispielsweise der Emittent von Bitcoin, Ether etc.? Können ein Algorithmus oder ein Code Rechtssubjekte sein? Diese Fragen sind nach wie vor weitgehend ungeklärt.

Bei Softwareprogrammen sind primär die Programmierer haftbar, wenn es möglich ist, ihnen einen Fehler und Verschulden gemäss den zivilrechtlichen Haftungsnormen nachzuweisen.[74] Das Programm selbst kann ja nicht unsorgfältig handeln, da es automatisch abläuft.

Intermediäre wie Cryptocurrency Exchanges, Wallet Provider etc. sind Rechtssubjekte, die man ebenfalls ins Recht fassen kann. Anwendbar sind allgemein gültige Normen wie das Datenschutzgesetz[75] und auf Verträge

---

69 KELLER/HESS, Rechtliche Anforderungen, S. 199.

70 Vgl. zum Folgenden KELLER/HESS, Rechtliche Anforderungen, S. 188 ff., 200.

71 FINMA-RS 2008/21; siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 189 ff.

72 Bestimmungen über die Datensicherheit: Art. 7 DSG, Art. 8 VDSG; siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 196 f., 201.

73 Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143 StGB); Verletzung des Fabrikations- oder Geschäftsgeheimnisses (Art. 162 StGB).

74 WEBER, Leistungsstörungen, S. 9 Abschnitt III.2.2.

75 ISLER, Datenschutz, passim.

das Zivilrecht sowie das Strafgesetzbuch.[76] Sehr oft sehen die anwendbaren Vertragsbestimmungen eine weitestgehende Freizeichnung vor:

> «*Participants therefore release and indemnify the provider from all liability for any loss that may occur as a result of their participation in the application and in connection with these risks.*»

Die Geltung solcher Klauseln wird durch die Ungewöhnlichkeitsregel eingeschränkt.[77] Die Ungewöhnlichkeitsregel läuft dort ins Leere, wo der Vertragspartner auf die an sich ungewöhnliche Klausel hingewiesen wurde und folglich von ihrem Inhalt Kenntnis genommen hat.[78]

Zumindest für Konsumenten stellt ein solch genereller Haftungsausschluss wohl einen Verstoss gegen Art. 8 UWG dar.[79] Eine Art. 8 UWG verletzende Klausel ist widerrechtlich (Art. 20 OR). Vertragsrechtlich kann Art. 8 UWG zur Nichtigkeit der betroffenen Klauseln führen.[80]

Sofern ein Haftungssubjekt bekannt ist, sollte die Haftung gemäss dem Prinzip der Risikosphären verteilt werden: Jede Partei übernimmt diejenigen Risiken, die aus ihrem Einflussbereich stammen, den sie am ehesten kontrollieren kann.[81] Das führt zur Haftung der Cryptocurrency Exchanges bei Verlust der Vermögenswerte ihrer Kunden, weil diese in der Hot Wallet verwahrt werden, welche gehackt wurde. Ebenso haften die Wallet-Betreiber, die Erschaffer von Applikationen, Programmen und Smart Contracts für die Mängel der von ihnen erschaffenen oder zur Verfügung gestellten Produkte.

Wie diese theoretische Haftbarkeit in der Praxis durchsetzbar ist, bleibt allerdings abzuwarten. Zu breit sind die Problemfelder[82] und zu unerfahren wohl viele Beteiligte.

---

76 WEBER, Leistungsstörungen, S. 8 f. Abschnitt III.2.1.

77 BGE 135 III 1 E. 2.1 S. 7; 138 III 411 E. 3.1 S. 412.

78 BGE 109 II 452 E. 5b S. 458; KOLLER, Auslegeordnung, S. 17 ff., 32 f.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 37 ff., 181.

79 Siehe dazu KELLER/HESS, Rechtliche Anforderungen, S. 199; KOLLER, Auslegeordnung, S. 17 ff.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 83 ff.

80 KOLLER, Auslegeordnung, S. 64 ff.; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 146 ff.

81 WIEGAND/MARTI, E-Banking Vereinbarung, S. 102; WIDMER, Missbräuchliche Geschäftsbedingungen, S. 202 ff.

82 Zur Frage des anwendbaren Rechts siehe HESS/SPIELMANN, Cryptocurrencies, S. 196 f.

VI. Zusammenfassung

Die zentralisierte Welt verfügt über ein differenziertes Regelwerk oder entsprechende Gerichtspraxis, welche bei nicht-autorisierten Transaktionen die Haftung und Schadloshaltung regeln.

In der dezentralen Welt überwiegt als Folge der Gleichung «code is law»[83] die faktische Durchsetzung gemäss der zugrundeliegenden Technologie gegenüber den gesetzlichen Normen oder der Gerichtspraxis. Die Verfügung mittels und über den Private Key ist endgültig, Autorisierung oder Nichtautorisierung hin oder her. Es zählt die Eigenverantwortung der InhaberInnen des Private Key.

Die gesetzlichen Vorschriften und die Gerichtspraxis beruhen seit jeher auf dem Faktischen. Das Recht wird der digitalen Realität Rechnung tragen, aber diese nicht als unabänderliche Wahrheit hinnehmen. Jurisprudenz bedeutet nach wie vor Abwägen von Interessen und Rechtsgütern:

> *«La proportionnalité est inhérente, en effet, à l'idée de justice, principe régulateur de tout droit.»*[84]

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 5. Mai 2018.

ALPEYEV PAVEL/NAKAMURA YUJI, How to Launder $500 Million in Digital Currency vom 29./31. Januar 2018, abrufbar unter: <https://www.bloomberg.com/news/articles/2018-01-29/how-to-launder-500-million-in-digital-currency-quicktake-q-a>.

ANTONOPOULOS ANDREAS M., Forkology: A Study of Forks for Newbies vom 24. Juni 2017, abrufbar unter: <https://www.youtube.com/watch?v=rpeceXY1QBM>.

ANTONOPOULOS ANDREAS M., Mastering Bitcoin:Unlocking Digital Cryptocurrencies, Sebastopol 2015.

BAJPAJ PRABLEEN, What Is Cold Storage For Bitcoin, abrufbar unter: <https://www.investopedia.com/articles/investing/030515/what-cold-storage-bitcoin.asp>.

BERGMANN CHRISTOPH, Das kleine 1x1 zur Bitcoin Cash Fork: Alles, was ihr wissen müsst vom 8. August 2017, abrufbar unter: <https://bitcoinblog.de/2017/08/08/das-kleine-1x1-zur-bitcoin-cash-fork-alles-was-ihr-wissen-muesst>.

83 LESSIG, Code Is Law, passim.

84 HUBER, Considérations, S. 417 ff., 423.

BERGMANN CHRISTOPH, Was passiert bei einem Hard Fork?vom 15. Juni 2015, abrufbar unter: <https://bitcoinblog.de/2015/06/15/was-passiert-bei-einem-hard-fork>.

BUIS ERIC, Das Stornorecht der Bank im Überweisungsverkehr, in: SZW 2002, S. 120–128.

CARSTENS AUGUSTIN, Money in the digital age: what role for central banks? Lecture of 6 February 2018 at the House of Finance, Goethe University, Frankfurt, abrufbar unter : <https://www.bis.org/speeches/sp180206.pdf>.

CASTOR AMY, A Short Guide to Bitcoin Forks vom 27. März 2017, abrufbar unter: <https://www.coindesk.com/short-guide-bitcoin-forks-explained>.

CZERNIK AGNIESZKA, Authentisierung, Authentifizierung und Autorisierung vom 24. Juni 2016, abrufbar unter: <https://www.datenschutzbeauftragter-info.de/authentisierung-authentifizierung-und-autorisierung>.

DECKER CHRISTIAN/WATTENHOFER ROGER, Information Propagation in the Bitcoin Network, 13-th IEEE International Conference on Peer-to-Peer Computing, 2013, abrufbar unter: <http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf>.

EMMENEGGER SUSAN, PSD2: Eckpunkte und Relevanz für Schweizer Finanzdienstleister, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Basel 2018, S. 17–66.

GIOVANOLI MARIO, Bargeld, Buchgeld, Zentralbankgeld: Einheit oder Vielfalt im Geldbegriff?, in: Festschrift für Beat Kleiner, Banken und Bankrecht im Wandel, Zürich 1993, S. 87–124.

GRÜNEWALD SERAINA, Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme (ZIK): Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 61, Zürich 2015, S. 93–112.

HERTIG ALYSSA, Rise of Replay Attacks Itensifies Ethereum Divide vom29/31. Juli 2016, abrufbar unter: <https://www.coindesk.com/rise-replay-attacks-ethereum-divide>.

HESS MARTIN, Euro-Zahlungen gemäss den SEPA-Rulebooks, insbesondere die Haftung der Banken, in Susan Emmenegger (Hrsg.), Cross-Border Banking, Basel 2009, S. 47–104.

HESS MARTIN/KALBERMATTER ANDRÉ/WEISS VOIGT ALEXANDRA, Kommentierung von Art. 81 FinfraG, in: Rolf Sethe/Olivier Favre/Martin Hess/Stefan Kramer/Ansgar Schott (Hrsg.), Schulthess-Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG, Zürich 2017.

HESS MARTIN/SPIELMANN PATRICK, Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht, in: Kapitalmarkt – Recht und Transaktionen XII, Zürich 2017, S. 145–202.

HESS MARTIN/STÖCKLI KATJA, Das Bucheffektengesetz aus der Optik des Kapitalmarktrechts, in: Kapitalmarktransaktionen V, Zürich 2010, S. 65–120.

HESS MARTIN/ZBINDEN ANDREA, Kommentierung von Art. 15 BEG, in: Dieter Zobl/Martin Hess/Ansgar Schott (Hrsg.), Kommentar zum Bucheffektengesetz (BEG), Zürich 2013.

HUBER MAX, Quelques considérations sur une révision éventuelle des Conventions de la Haye relatives à la guerre, in: Revue Internationale de la Croix Rouge, 37 (439)/ 1955, S. 417–433.

ISLER MICHAEL, Datenschutz auf der Blockchain, in: Jusletter 4. Dezember 2017.

KELLER CLAUDIA/HESS MARTIN, Rechtliche Anforderungen an System- und Datensicherheit und Compliance für webbasierte und mobile Zahlungen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, (ZIK): Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 61, Zürich 2015, S. 181-205.

KOLLER THOMAS, Art. 8 UWG: Eine Auslegeordnung, in: Susan Emmenegger (Hrsg), Das Bankkonto, Basel 2013, S. 17–81.

LESSIG LAWRENCE, Code Is Law, On Liberty in Cyberspace, in: Harvard Magazine 29 February 2012, abrufbar unter: <https://harvardmagazine.com/2000/01/code-is-law-html>.

NAKAMOTO SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, abrufbar unter: <https://bitcoin.org/bitcoin.pdf>.

ROSIC AMEER, Paper Wallet Guide: How to Protect Your Cryptocurrency, 2017, abrufbar unter: <https://blockgeeks.com/guides/paper-wallet-guide>.

ROSIC AMEER, Proof of Work vs. Proof of Stake: Basic Mining Guide, 2017, abrufbar unter: <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake>.

SONG JIMMY, Replay Attacks Explained vom 21. August 2017, abrufbar unter: <https://bitcointechtalk.com/replay-attacks-explained-e3d6d2ea0ab2>.

SZABO NICK, Trusted Third Parties Are Security Holes, originally published in 2001, abrufbar unter: <http://nakamotoinstitute.org/trusted-third-parties/#selection-7.6-17.34>.

THOMA JÖRG, Sound Wallet. Private Schlüssel, auf Schallplatte gepresst vom 5. September 2014, abrufbar unter: <https://www.golem.de/news/sound-wallet-private-schluessel-auf-schallplatte-gepresst-1409-109073.html>.

ULM BOGDAN, Listen to your Bitcoins with Sound Wallet vom 2. September 2014, abrufbar unter: <https://cointelegraph.com/news/listen-to-your-bitcoins-with-sound-wallet>.

WEBER ROLF H., Kommentierung von Art. 27 und 28 BEG, in: ZOBL DIETER/HESS MARTIN/SCHOTT ANSGAR, Kommentar zum Bucheffektengesetz (BEG), Zürich, 2013.

WEBER ROLF H., Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, in: Jusletter 4. Dezember 2017.

WELTER PATRICK, Hackerangriff trifft japanische Krypto-Börse vom 29. Januar 2018, abrufbar unter: <https://www.nzz.ch/wirtschaft/hackerangriff-trifft-japanische-krypto-boerse-ld.1352017>.

WIDMER ESTHER, Missbräuchliche Geschäftsbedingungen nach Art. 8 UWG (Diss. Bern), Zürich 2015.

WIEGAND WOLFGANG/MARTI MARIO, Die E-Banking-Vereinbarung – Rechtliche Einordnung und Wirkung, in: E-Banking, Die einzelnen Rechtsgeschäfte, Berner Bankrechtstag BBT, Band 9/2002, Bern 2002, S. 75–108.

YOUNG JOSEPH, BitGrail Vs. Nano: Who Is Responsible For the $150 Million Theft? vom 18. Februar 2018, abrufbar unter: <https://cointelegraph.com/news/bitgrail-vs-nano-who-is-responsible-for-the-150-million-theft>.

ZELLWEGER-GUTKNECHT CORINNE, Digitale Landeswährung – Ein Überblick, in: Jusletter vom 31. Oktober 2016.

Zahlung und Verzug bei virtuellen Währungen

Harald Bärtschi/Nicolas Jacquemart/Stephan D. Meyer, Zürich*

Inhaltsverzeichnis

* Harald Bärtschi, Prof. Dr. iur., Titularprofessor für Privat- und Wirtschaftsrecht der Universität Zürich, Leiter des Zentrums für Unternehmens- und Steuerrecht der ZHAW School of Management and Law, Rechtsanwalt bei Bärtschi Rechtsanwälte AG; Nicolas Jacquemart, M.A. HSG in Law, Rechtsanwalt; Stephan D. Meyer, MLaw, LL.M.; letztere beiden sind Doktoranden der Universität Zürich und arbeiten an der ZHAW School of Management and Law im interdisziplinären Projekt des Schweizerischen Nationalfonds über virtuelle Währungen (Projekt-Nr. 10001A_162442). Die Verfasser äussern ihre persönliche Meinung.

I. Zahlung in virtueller Währung

1. Fragestellung

In einer von der Computertechnik geprägten Welt wird auch das Geld zunehmend digitalisiert. Was vor Jahrzehnten mit der Abwicklung von Buchgeldtransaktionen zwischen Banken auf informationstechnischer Basis begonnen hat, wird heute mit Bitcoin und ähnlichen virtuellen Währungssystemen fortgesetzt. Die bislang prominentesten Wegbereiter dieser Entwicklung koppeln sich bewusst vom Konzept staatlich anerkannter Währungen ab und bilden eigene Systeme. Nachdem sich das Geld bereits weitgehend von seiner traditionellen Qualifikation als Sache gelöst hat,[1] droht es nun in seiner virtuellen Spielart auch noch die «institutionellen» Schranken zu durchbrechen und seiner staatlichen Grundlage verlustig zu gehen. Doch wittern auch Regierungen und Zentralbanken eine Chance, sodass Bestre-

[1] Vgl. BK OR-WEBER, Art. 84 N 13.

bungen einzelner Staaten im Gang sind, ihrerseits virtuelle Währungen herauszugeben oder zumindest anzuerkennen.[2]

Das Zivilrecht der Schweiz basiert noch auf einer vordigitalen Konzeption der Zahlungsvorgänge. Die Anwendung der «analogen» Regeln auf digitale Sachverhalte wirft komplexe Fragen auf. Um Zahlungsvorgänge in virtueller Währung zivilrechtlich einordnen zu können, sind zunächst die Begriffe Geld und Geldschuld, Währung, Zahlungsmittel, Zahlung und virtuelle Währung zu umschreiben (I.2). Nach einem kurzen Überblick über die technische Abwicklung eines Zahlungsvorgangs in virtueller Währung (I.3) wird untersucht, ob eine Schuld in virtueller Währung als Geldschuld im Sinne des Obligationenrechts[3] betrachtet werden kann, welches die rechtlichen Folgen sind und inwieweit die staatliche Anerkennung einer virtuellen Währung eine Rolle spielt (I.4). Die erheblichen Kursschwankungen werfen die Frage auf, ob eine Schuld in virtueller Währung nachträglich in der Höhe angepasst werden kann. Ausgewählte Modalitäten der Erfüllung einer Schuld in virtueller Währung, namentlich die Möglichkeit, die Schuld in einer anderen Währung zu erfüllen (I.5.a), sowie der Zeitpunkt (I.5.b) und der Ort der Erfüllung (I.5.c), bilden den Abschluss des Kapitels zur Zahlung in virtueller Währung. Es folgen Ausführungen zum Institut der Verrechnung (II) und zu Leistungsstörungen mit Fokus auf dem Verzug, der Unmöglichkeit und Schadenersatzansprüchen (III). Mit der Verzugsthematik zusammen hängt die Frage der Behandlung von Forderungen in virtueller Währung im Vollstreckungsrecht (IV). Der Beitrag schliesst mit einem Fazit (V).

[2] Teilweise werden staatlich herausgegebene «virtuelle Währungen» terminologisch nicht als solche qualifiziert, vgl. hinten, bei Fn. 49.

[3] Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220, «OR»).

2. Terminologie

a) Geld und Geldschuld

aa) Geld

Für das schweizerische Privatrecht existiert keine Legaldefinition des Geldes oder der Geldschuld, und die Lehre äussert sich uneinheitlich.[4] Der Ausdruck wird im Obligationenrecht verschiedentlich erwähnt, etwa in Art. 47 und Art. 49 OR («Geldsumme» als Genugtuung), Art. 74 Abs. 2 Ziff. 1 OR (Erfüllungsort für «Geldschulden»), Art. 84 Abs. 1 OR (Erfüllung von «Geldschulden»), Art. 104 Abs. 1 OR (Verzugszins bei «Geldschuld») oder Art. 323*b* Abs. 1 OR («Geldlohn»). Daneben spielt der Begriff bei der Auslegung von weiteren Bestimmungen eine Rolle, so wenn das Gesetz von «Zahlung», «zahlen» oder von «Preis» spricht.[5]

Die herrschende Lehre orientiert sich terminologisch an den Funktionen des Geldes. Der physische oder digitale «Träger», sei er nun eine Münze, eine Banknote oder ein digitaler Token, wird Geld genannt, wenn er Geldfunktionen ausübt.[6] Körperlichkeit wird nicht vorausgesetzt. Digitale Werteinheiten sind gemäss diesem funktionalen Verständnis dann Geld, wenn sie sich als allgemeines Tausch- beziehungsweise Zahlungsmittel einsetzen lassen und als Wertmesser für Güter sowie Dienstleistungen, das heisst als abstrakte Rechnungseinheit, dienen können.[7] Je nach dem wirtschaftlichen und gesellschaftlichen Umfeld können sich die Funktionen wandeln, sodass der funktionale Geldbegriff nicht statisch ist.

Die Lehre unterscheidet zwischen Geld in engerem und in weiterem Sinne.[8] *Geld in engerem Sinne* erfasst die gesetzlichen Zahlungsmittel, die von einem Staat als solche anerkannt sind[9] und von der Gläubigerin, wenn der Schuldner die Zahlung erbringt, kraft Gesetzes zum Nennwert akzeptiert

---

4 Vgl. BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 142 f.; EGGEN, Jusletter 4. Dezember 2017, Rz. 5 ff.; BSK OR-LEU, Art. 84 N 2; ZK OR-SCHRANER, Art. 84 N 3 ff.; BK OR-WEBER, Art. 84 N 5 und 9 ff.

5 ZK OR-SCHRANER, Art. 84 N 25; BK OR-WEBER, Art. 84 N 68.

6 BK OR-WEBER, Art. 84 N 15 (Geld ist, was als Geld fungiert).

7 Zum Ganzen ZK OR-SCHRANER, Art. 84 N 4; BK OR-WEBER, Art. 84 N 49 und 63 ff. m.w.H.; WEBER, Elektronisches Geld, S. 30; enger die verfassungsrechtliche Umschreibung in der Botschaft Währungsartikel, S. 4029 (vom Staat als Zahlungsmittel anerkanntes Geld).

8 ZK OR-SCHRANER, Art. 84 N 6 ff.; BK OR-WEBER, Art. 84 N 30.

9 Botschaft Währungsartikel, S. 4029.

werden müssen. *Geld in weiterem Sinne* hat die Gläubigerin gestützt auf eine ausdrückliche oder stillschweigende Vereinbarung als Entgelt anzunehmen. Die Rede ist auch von usuellem beziehungsweise Verkehrsgeld oder von faktischen Zahlungsmitteln. Beispiele sind Bargeld in einer Fremdwährung oder Buch- und elektronisches Geld in einer staatlich anerkannten Währung. Auch die Komplementärwährung WIR der Basler WIR Bank Genossenschaft lässt sich unter den weiten Geldbegriff subsumieren.[10] Den meisten Bestimmungen des Schweizer Privatrechts, welche sich mit Geld befassen, liegt der weite Begriff zugrunde.[11]

bb) Geldschuld

Mit dem Begriff des Geldes in Zusammenhang steht die Geldschuld. Wie aus Art. 84 Abs. 1 OR hervorgeht, lauten Geldschulden gemäss der Vorstellung des Gesetzgebers auf eine gewisse Währung, für welche gesetzliche Zahlungsmittel existieren. Davon wird ein bestimmter oder bestimmbarer Betrag geschuldet. Der Schuldner erfüllt seine Geldschuld, indem er der Gläubigerin gesetzliche Zahlungsmittel in der geschuldeten Höhe verschafft, wobei er mangels gegenteiliger Vereinbarung die Art der gesetzlichen Zahlungsmittel auswählen darf.[12] Aus Art. 2 WZG[13] ergibt sich, dass eine auf Schweizer Franken lautende Geldschuld – ausser zwischen Inhabern eines Girokontos bei der Nationalbank – grundsätzlich in bar zu erfüllen ist, nämlich in Münzen oder Banknoten. Die Gläubigerin ist umgekehrt gehalten, die vom Schuldner angebotenen Zahlungsmittel zu akzeptieren.[14] Ansonsten gerät sie in Annahmeverzug. Mangels gegenteiliger Abrede oder Übung ist die Gläubigerin nicht verpflichtet, Buchgeld, WIR, Checks oder sonstige alternative Formen des Geldes in weiterem Sinne zu akzeptieren.[15]

---

10 ZK OR-SCHRANER, Art. 84 N 8 und 18 ff.; BK OR-WEBER, Art. 84 N 61 f. (usueller Geldcharakter innerhalb der WIR-Teilnehmer, aber kein Geld im Sinne von Art. 104 Abs. 1 OR).

11 BSK OR-LEU, Art. 84 N 2.

12 ZK OR-SCHRANER, Art. 84 N 141; BK OR-WEBER, Art. 84 N 130.

13 Bundesgesetz über die Währung und die Zahlungsmittel (WZG) vom 22. Dezember 1999 (SR 941.10).

14 Für Münzen statuiert Art. 3 Abs. 1 Satz 1 WZG eine begrenzte Annahmepflicht, indem die Gläubigerin «bis zu 100 schweizerische Umlaufmünzen an Zahlung zu nehmen» hat. Schweizerische Banknoten und auf Franken lautende Sichtguthaben müssen nach Art. 3 Abs. 2 und Abs. 3 WZG unbeschränkt zur Zahlung angenommen werden.

15 ZK OR-SCHRANER, Art. 84 N 155 ff.

Aufgrund der dispositiven Natur von Art. 84 Abs. 1 OR ist es den Parteien unbenommen, die Tilgung einer Geldschuld statt in bar beispielsweise mittels elektronischer Überweisung auf das Bankkonto der Gläubigerin zuzulassen oder vorzuschreiben. Es handelt sich gleichwohl um die Erfüllung einer Geldschuld und nicht bloss um eine Leistung an Zahlungs statt.[16] Es steht den Parteien auch frei, für eine Geldschuld anstelle der gesetzlich vorgesehenen Betragsschuld (Summenschuld) eine Stückschuld – etwa die Verschaffung individuell ausgewählter Banknoten – oder eine Gattungsschuld (Geldsortenschuld) – zum Beispiel die Leistung ausschliesslich in Einfrankenstücken – zu vereinbaren.[17] Die Qualifikation ist relevant, falls die für die Leistung vorgesehenen Geldstücke vor der Übergabe an die Gläubigerin zerstört werden.

cc) Eigenschaften der Geldschuld

Auch wenn die Geldschuld im Obligationenrecht nicht direkt definiert wird, haben Lehre und Rechtsprechung gewisse Merkmale einer Geldschuld entwickelt, welche sich zum Teil aus der gesetzlichen Regelung ableiten lassen, bisweilen aber auch einer Grundlage im Obligationenrecht entbehren.

Eine zentrale, nicht ausdrücklich im Gesetz statuierte Eigenschaft der Geldschuld wird durch das *Nennwertprinzip* (Nominalismus) ausgedrückt: Danach ist eine Geldschuld grundsätzlich in gesetzlichen Zahlungsmitteln im ziffernmässig festgesetzten Betrag zu erfüllen, wobei der Betrag bei Entstehung der Schuld massgeblich bleibt.[18] Verändert sich der Geldwert bis zum Zeitpunkt der Erfüllung der Schuld, hat dies auf den Umfang der Leistungspflicht keinen Einfluss. So trägt die Gläubigerin das Risiko einer Geldentwertung. Dieser Grundsatz gilt aus Sicht des Schweizer Rechts auch für Fremdwährungsschulden.[19] Kollisionsrechtlich ist jeweils das auf die Schuld anwendbare Recht (Schuldstatut) massgeblich, nicht das Währungsstatut.[20] Durchbrochen wird das Nennwertprinzip durch gesetzlich vorgesehene oder vertraglich vereinbarte Indexierungen sowie durch wertbeständige

16 Botschaft WZG, S. 7271 f.

17 ZK OR-SCHRANER, Art. 84 N 144 ff.; BK OR-WEBER, Art. 84 N 135 ff.

18 Dazu ZK OR-SCHRANER, Art. 84 N 73 ff.; BK OR-WEBER, Art. 84 N 179 ff. Das Gegenteil zum Nennwertprinzip ist die Kurswerttheorie (Valorismus), wonach die Geldschuld im Erfüllungszeitpunkt an die eingetretene Entwicklung der Kaufkraft anzupassen ist.

19 ZK OR-SCHRANER, Art. 84 N 78; BK OR-WEBER, Art. 84 N 320.

20 Art. 147 Abs. 2 Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987 (SR 291); Botschaft IPRG, S. 435.

Schulden (Geldwertschulden). Letztere lauten zunächst nicht auf einen fixen Betrag und gewähren zum Beispiel bei einer Schadenersatzleistung der Gläubigerin einen Wertausgleich im Erfüllungs- beziehungsweise Urteilszeitpunkt.[21]

Entgegen dem Nennwertprinzip ist ausnahmsweise eine nachträgliche Wertanpassung durch das Gericht gestützt auf Art. 2 ZGB[22] gemäss der *clausula rebus sic stantibus* denkbar, so bei einem unvorhersehbaren Währungszerfall, welcher nach dem Vertragsschluss eine gravierende Äquivalenzstörung bewirkt, nicht hingegen bei einer schleichenden Geldentwertung.[23]

Ein weiteres Merkmal einer Geldschuld ist – getreu dem Schlagwort «Geld muss man haben.» – der Umstand, dass ein Mangel an Geld beim Schuldner nicht als Unmöglichkeit betrachtet wird. Die Durchsetzung einer Geldschuld gegen einen Schuldner bleibt auf dem Schuldbetreibungsweg stets möglich, unter dem Vorbehalt der unpfändbaren Vermögenswerte (Art. 92 SchKG[24]) und des bloss beschränkt pfändbaren Einkommens (Art. 93 SchKG).

b) Währung

«Währung» beziehungsweise «Währungseinheit» meint nicht das konkrete Zahlungsmittel, zum Beispiel eine Zehn-Pfund-Note, sondern bezeichnet im internationalen Geldverkehr die abstrakte Rechnungs- und Standardwerteinheit,[25] und zwar typischerweise in Gestalt einer staatlich anerkannten, gesetzlich festgesetzten Ausprägung, etwa US-Dollar oder Euro.[26] Nach dem bisherigen Verständnis bezieht sich eine Währung auf das Geldwesen und die Zahlungsmittel eines Staates, verstanden als Völkerrechtssubjekt. Folglich ist die Qualifikation als Währung mit Unsicherheiten behaftet, soweit zweifelhaft ist, ob eine Gebietskörperschaft völkerrechtlich als eigenständiger Staat gelten kann. Erwähnt sei etwa der Neue Taiwan-Dollar von «Tai-

21 BSK OR-LEU, Art. 84 N 5; ZK OR-SCHRANER, Art. 84 N 80 ff.; BK OR-WEBER, Art. 84 N 196 ff.

22 Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210).

23 Die einschlägigen Gerichtsurteile der 1920er- und 1930er-Jahre wurden allerdings nicht mit der *clausula rebus sic stantibus* begründet, vgl. hinten, bei Fn. 93.

24 Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) vom 11. April 1889 (SR 281.1).

25 Botschaft Währungsartikel, S. 4030.

26 ZK OR-SCHRANER, Art. 84 N 55.

wan (Chinesisches Taipei)».[27] Mit dem Aufkommen virtueller Währungen, welche gesetzlich geregelt, staatlich anerkannt oder sogar als Haupt– beziehungsweise Nebenwährung durch eine Regierung oder Zentralbank herausgegeben werden, steigt der Klärungsbedarf, wann eine Währung vorliegt. Wiederum ist es problematisch, eine abstrakte, von konkreten Gesetzesbestimmungen losgelöste terminologische Einordnung vorzunehmen.

Für den Begriff der Währung im Bereich des Obligationenrechts[28] verweist Art. 147 Abs. 1 IPRG auf das öffentliche[29] «Recht des Staates, dessen Währung in Frage steht» *(lex monetae)*. Währung meint die gesetzlich anerkannten Zahlungsmittel.[30] Die Norm dürfte auch in Fällen mit internationalem Bezug anwendbar sein, wenn Gläubigerin und Schuldner im gleichen Staat Sitz oder Wohnsitz haben.[31] Für die Bestimmung der hiesigen Währung sind somit die Vorschriften des öffentlichen Währungsrechts massgeblich. Gemäss Art. 1 WZG ist die schweizerische Währungseinheit der Franken, eingeteilt in 100 Rappen. Darauf beziehen sich das Buchgeld der Banken und weitere Geldformen.

Die Regelung von Art. 147 Abs. 1 IPRG bestätigt, dass eine Währung gemäss der Vorstellung des schweizerischen Gesetzgebers von einem *Staat* herausgegeben wird und eine rechtliche Grundlage hat. Folglich stellt WIR keine Währung dar, wie auch die Allgemeinen Geschäftsbedingungen der WIR Bank Genossenschaft ausdrücklich festhalten.[32] Analog auf eine nicht staatlich geschaffene «Währung» angewandt, würde Art. 147 Abs. 1 IPRG

---

27 Offizielle Bezeichnung gemäss der Liste der Staatenbezeichnungen der Direktion für Völkerrecht des Eidgenössischen Departements für auswärtige Angelegenheiten, Fassung vom 6. Februar 2018 (<www.eda.admin.ch/dam/eda/de/documents/aussenpolitik/voelkerrecht/liste-etats_DE.pdf>). Der Schweizer Bundesrat hat die Republik China (Taiwan) nicht anerkannt.

28 Vgl. die Überschrift zum 9. Kapitel (Art. 112 ff. IPRG).

29 Vgl. Art. 13 Satz 2 IPRG, wonach die Anwendbarkeit einer Bestimmung des ausländischen Rechts nicht dadurch ausgeschlossen ist, dass ihr ein öffentlich-rechtlicher Charakter zugeschrieben wird.

30 BSK IPRG-DASSER, Art. 147 N 5.

31 Zu den unterschiedlichen Lehrmeinungen BSK IPRG-DASSER, Art. 147 N 3. Nach einzelnen Autoren genügt es, dass in einem Binnenschuldverhältnis Geld in Fremdwährung geschuldet ist.

32 Allgemeine Geschäftsbedingungen der WIR Bank Genossenschaft vom 1. Januar 2017 (AGB WIR), Ziff. C.1 («WIR gelten nicht als Fremdwährung»); ebenso die Bedingungen der Teilnahme am WIR-Netzwerk vom Januar 2017 (Teilnahmebedingungen WIR), Ziff. 1.

auf das *private* Regelwerk verweisen, welches dieser «Währung» zugrunde liegt.

In welcher Währung eine geschuldete Zahlung zu leisten ist, ergibt sich zumeist aus den Umständen oder ist von den Parteien ausdrücklich festgelegt worden. Die Bestimmung der Währung untersteht gemäss Art. 147 Abs. 3 IPRG dem Recht des Staates, in welchem die Zahlung zu erfolgen hat (Zahlungsstatut). Massgeblich ist der nach dem Schuldstatut durch Vertrag oder Gesetz bestimmte, nicht der tatsächliche Zahlungsort.[33] Geht es etwa um die Kaufpreiszahlung aus einem internationalen Vertrag, welcher Schweizer Recht untersteht, an eine Verkäuferin mit Wohnsitz in der Schweiz, liegt der Zahlungsort mangels abweichender Vereinbarung in der Schweiz (Art. 74 Abs. 2 Ziff. 1 OR). Dies führt für die Bestimmung der akzeptierten Währung, zumindest sofern tatsächlich in der Schweiz bezahlt wird, zur Anwendung von Art. 84 Abs. 2 OR (hinten, Kap. I.5.a).

c) Zahlungsmittel

Vom Begriff des Geldes und der Währung abzugrenzen ist das Zahlungsmittel. Letzteres erfasst einerseits funktional alle Mittel, welche sich für die allgemeine Verwendung als Entgelt beim Erwerb von Gütern oder Dienstleistungen eignen, und bezeichnet in der Schweiz anderseits – verstanden als *gesetzliches* Zahlungsmittel – das hier staatlich anerkannte Geld gemäss Art. 2 WZG, nämlich Münzen, Banknoten und zwischen Inhabern von entsprechenden Girokonten die auf Franken lautenden Sichtguthaben bei der Schweizerischen Nationalbank.[34] Ist eine andere Währung als der Schweizer Franken geschuldet, bestimmen sich die gesetzlichen Zahlungsmittel aufgrund von Art. 147 Abs. 1 IPRG (vorne, bei Fn. 30) nach der ausländischen Rechtsordnung.

Die staatliche Festsetzung der gesetzlichen Zahlungsmittel mit beschränkter beziehungsweise unbeschränkter Annahmeobliegenheit seitens der Gläubigerin gewährt dem Rechtsverkehr die Sicherheit, eine Geldschuld durch Übertragung von Geld in Form der gesetzlichen Zahlungsmittel tilgen zu können, soweit keine anderweitige Abrede besteht.[35] Die Sichtguthaben bei der Schweizerischen Nationalbank sind als Sonderform von Buchgeld

---

33 Botschaft IPRG, S. 436.

34 Vgl. vorne, nach Fn. 12; zum letzteren Aspekt Botschaft WZG, S. 7263.

35 Botschaft WZG, S. 7261; näher zum Annahmezwang der Gläubigerin ZK OR-SCHRANER, Art. 84 N 59 ff.; BK OR-WEBER, Art. 84 N 142 ff.

ohne Solvenzrisiko ein gesetzliches Zahlungsmittel im elektronischen Interbank-Zahlungsverkehr SIC.[36] Keine gesetzlichen Zahlungsmittel sind das Buchgeld der Banken in Form von Kontoguthaben der Kunden, Debit- oder Kreditkartenguthaben und sonstige elektronische Zahlungsmittel.[37] Nichtsdestotrotz sind diese Erscheinungsformen als Geld in weiterem Sinne zu qualifizieren. Angesichts der unterschiedlichen Verwendung weist der Begriff des Zahlungsmittels somit keine einheitliche Struktur auf.

d) Zahlung

Im Obligationenrecht wird die Zahlung in Art. 84–90 OR geregelt. Sie ist nach dem Verständnis des Gesetzgebers die Erfüllung (Art. 68 ff. OR) einer Geldschuld «in gesetzlichen Zahlungsmitteln der geschuldeten Währung» (Art. 84 Abs. 1 OR).[38] Umgangssprachlich ist bei der Leistung eines Entgelts – zumeist in einer verbreiteten, staatlich anerkannten Währung – für den Bezug von Gütern oder Dienstleistungen von «Zahlung» die Rede. Ob es sich beim zugrunde liegenden Vertrag um einen Kauf-, Miet-, Arbeits- oder Werkvertrag beziehungsweise einen Auftrag handelt, ist kaum von Bedeutung. Der Vertragstyp hat grundsätzlich keinen Einfluss auf die Art der geschuldeten Zahlung. Umgekehrt stellt die Zahlung in der Regel nicht die für den Vertrag charakteristische Leistung dar.[39] Im Kollisionsrecht zeigt sich dies am Katalog in Art. 117 Abs. 3 IPRG. Das Obligationenrecht verwendet für die Erfüllung von Geldschulden neben «Zahlung» verschiedene andere Begriffe.[40] Art. 184 Abs. 1 OR erwähnt die Bezahlung des Kaufpreises, Art. 253 OR die Leistung eines Mietzinses, Art. 319 Abs. 1 OR die Entrichtung eines Lohns und Art. 363 beziehungsweise Art. 394 Abs. 3 OR die Leistung einer Vergütung. Beim Darlehen (Art. 312 OR) und beim Anweisungsverhältnis (Art. 466 OR), bei welchem die Geldleistung das Rechtsverhältnis prägt, verwendet der Gesetzgeber die Wendung «Übertragung des Eigentums an einer Summe Geldes» beziehungsweise Leistung von Geld. Das

---

36 Botschaft WZG, S. 7270 f.; Botschaft Währungsartikel, S. 4029.

37 Botschaft WZG, S. 7271. Dies bedeutet, dass eine Gläubigerin mangels gegenteiliger Abrede nicht die Erfüllung einer Geldschuld durch Gutschrift auf ihr Bankkonto verlangen darf.

38 Mit dem Inkrafttreten des WZG am 1. Mai 2000 ist Art. 84 OR angepasst worden, vgl. Botschaft WZG, S. 7285. Gemäss dem früheren Wortlaut von Art. 84 Abs. 1 OR waren Geldschulden «in Landesmünze» zu bezahlen.

39 ZK OR-SCHRANER, Art. 84 N 3; BK OR-WEBER, Art. 84 N 5.

40 Vgl. KÜNG, Zahlung und Zahlungsort, S. 23 m.w.H.

Wechsel- und das Checkrecht (Art. 990 ff. beziehungsweise Art. 1100 ff. OR) sprechen durchgängig von «Zahlung».

Welche Art von Zahlung oder Entgelt noch unter den gesetzlichen Vertragstyp subsumiert werden kann, hängt von der Vertragsart ab. Ein Sonderfall stellt die «Zahlung» in WIR dar. Darauf ist zurückzukommen (hinten, I.5.a.bb). Bei virtuellen Währungen fragt sich, ob deren Übertragung eine Zahlung im Sinne von Art. 84 OR darstellt.

e) Virtuelle Währung

aa) Umschreibung

Als virtuelle Währung wird ein System aus Werteinheiten bezeichnet, welche digital geschaffen sowie verwaltet werden und für die Verwendung als Zahlungs- oder Tauschmittel konzipiert sind.[41] Nach Auffassung des Bundesrats und der Eidgenössischen Finanzmarktaufsicht FINMA ist eine virtuelle Währung eine digitale Darstellung eines Werts mit eigener Denomination; sie ist im Internet handelbar und übernimmt die Funktion von Geld, das heisst sie kann als Zahlungsmittel für Güter und Dienstleistungen verwendet werden, ohne als gesetzliches Zahlungsmittel akzeptiert zu sein.[42] Von elektronischem Geld in herkömmlichem Sinne unterscheidet sich die virtuelle Währung dadurch, dass sie nicht mit gesetzlichen Zahlungsmitteln unterlegt ist. Diese Definition des Bundesrats und der FINMA ähnelt derjenigen der *Financial Action Task Force/Groupe d'action financière* (FATF/GAFI).[43] Indessen darf der Begriff aufgrund der unterschiedlichen Ausrichtung nicht unbesehen von der Geldwäschereibekämpfung auf das Zivilrecht übertragen werden.[44] Eine einheitliche und exakte Definition ist aus rechtlicher Sicht weder möglich noch sinnvoll. Es liessen sich daraus auch kaum juristische Folgerungen ableiten. Die Erscheinungsformen sind vielfältig und reichen von Computerspielen (zum Beispiel Gold in World of Warcraft oder

41 Vgl. BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 115 m.w.H.

42 Bericht virtuelle Währungen, S. 7 f.; Erläuterungsbericht FINMA, S. 11.

43 Vgl. FATF, Guidance for a risk-based approach to virtual currencies vom Juni 2015, S. 26, worin der Ausdruck «*virtual currency*» definiert wird als «digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction».

44 Vgl. BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 140.

Linden Dollars in Second Life) bis zu Kundenkarten (etwa Superpunkte oder Payback Points).

Als Unterkategorie der virtuellen Währungen findet der Begriff der *Kryptowährungen* zunehmend Verbreitung. Darunter werden Systeme aus Werteinheiten verstanden, welche durch den Einsatz kryptografischer Verschlüsselungstechniken hohen Sicherheitsbedürfnissen genügen.

bb) Kategorien virtueller Währungen

Angesichts der vielfältigen Erscheinungsformen sind für die virtuellen Währungen gewisse Klassifikationen vorgeschlagen worden. Zwei davon sollen hier behandelt werden, bevor näher auf die zivilrechtliche Erfassung eingegangen wird.

Die Unterscheidung zwischen offenen, umtauschbaren *(convertible)* und geschlossenen, nicht-umtauschbaren *(non-convertible)* virtuellen Währungen richtet sich nach der faktischen und nicht etwa rechtlichen Möglichkeit, Einheiten einer virtuellen Währung in solche einer staatlichen Währung zu wechseln.[45] Von Bedeutung ist, ob ein – wenn auch womöglich inoffizieller oder gar vom Währungssystembetreiber unerlaubter – Markt für die virtuelle Währung existiert oder nicht. Idealerweise sind virtuelle Währungen frei in traditionelle staatliche Währungen oder in andere virtuelle Währungen umtauschbar. Beispiele hierfür sind Bitcoin oder Ether, welche über diverse Plattformen und Automaten gewechselt werden können.

Eine zweite Unterscheidung ist diejenige zwischen zentralen *(centralized)* und dezentralen *(decentralized)* virtuellen Währungen.[46] Eine zentrale virtuelle Währung wird von einer zentralen Instanz ausgegeben, verwaltet und gesteuert. Dezentral ist eine virtuelle Währung, wenn sie im dezentralen Computer-Netzwerk (*Peer-to-Peer*-Netzwerk) durch nicht miteinander besonders verbundene Teilnehmer ausgegeben, verwaltet und gesteuert wird. Die dezentrale Datenverwaltung kommt im Ausdruck *distributed ledger technology* anschaulich zur Geltung. Die klassischen Kryptowährungen basieren zumeist auf Open-Source-Software und werden in einem dezentralen Computer-Netzwerk abgebildet. Doch könnten Kryptowährungen auf ähnlicher technischer Grundlage auch zentral, beispielsweise durch eine staatliche Regierung, Zentralbank oder private Institution, ausgegeben werden.

45 FATF (Fn. 43), S. 26 f.

46 FATF (Fn. 43), S. 27.

Soweit nicht anders vermerkt, orientieren sich die Ausführungen dieses Beitrags in der Regel an umtauschbaren Kryptowährungen im umschriebenen Sinne, selbst wenn der allgemeinere Begriff der virtuellen Währungen verwendet wird. Zumeist geht es um dezentrale virtuelle Währungen, doch werden verschiedentlich auch zentrale virtuelle Währungen behandelt.

cc) Gesetzliche Regelung virtueller Währungen

Ausdrücklich angesprochen werden virtuelle Währungen in der Schweizer Finanzmarkgesetzgebung: Seit einigen Jahren umfasst die «Geld- und Wertübertragung» gemäss Art. 2 lit. c GwV-FINMA[47] beziehungsweise das «Geld- oder Wertübertragungsgeschäft» im Sinne von Art. 4 Abs. 2 GwV[48] auch den Transfer von Vermögenswerten durch Entgegennahme von virtuellen Währungen und Auszahlung oder Überweisung einer entsprechenden Summe.

dd) Staatlich herausgegebene virtuelle Währungen

Zum Teil werden staatlich herausgegebene virtuelle Währungen nicht als solche betrachtet.[49] Wird eine virtuelle Währung durch einen Staat herausgegeben und lautet diese auf die bestehende Landeswährung, wäre es in der Tat missverständlich, von einer eigenen virtuellen Währung zu sprechen. In einem solchen Fall liegt bloss eine alternative technische Erscheinungsform der existierenden Währung vor, wie bei E-Geld, welches auf Franken lautet. Insoweit rechtfertigt sich aus Schweizer Sicht eine Qualifikation als normale Fremdwährung.

Aber auch bei einer separaten Währung, welche durch einen Staat digital herausgegeben wird, liegt es nahe, diese wie eine traditionelle Fremdwährung zu behandeln. Weniger eindeutig ist die Situation, wenn der Staat lediglich eine bestehende virtuelle Währung als Zahlungsmittel anerkennt. Erforderlich ist jedenfalls eine materiell-rechtliche Prüfung; die rechtliche Beurteilung sollte nicht von der Definition virtueller Währungen abhängen.

---

47 Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (Geldwäschereiverordnung-FINMA, GwV-FINMA) vom 3. Juni 2015 (SR 955.033.0).

48 Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung, GwV) vom 11. November 2015 (SR 955.01).

49 Vgl. EZB-Stellungnahme, Ziff. 1.1.3.

Auf den Sonderfall der staatlichen Herausgabe beziehungsweise Anerkennung ist daher zurückzukommen (hinten, I.4.d).

ee) Wertstabilisierte virtuelle Währungen

Verbreitete virtuelle Währungen wie Bitcoin und Ether unterliegen starken Wertschwankungen.[50] Die hohe Volatilität stellt für die praktische Nutzung und Verbreitung virtueller Währungen ein erhebliches Problem dar. Die Volatilität beeinträchtigt die Einsatzmöglichkeit als Zahlungsmittel und fördert die Verwendung als spekulatives Anlageinstrument, was nicht der ursprünglichen Idee virtueller Währungen entspricht. Deshalb wird versucht, virtuelle Währungen mit einer erhöhten Wertstabilität zu schaffen, häufig mittels Anbindung der virtuellen an eine staatliche Währung. Insoweit stellt die virtuelle Währung einen Ersatz für die entsprechende staatliche Währung dar. Solche virtuellen Währungen werden als *stable coins* bezeichnet.[51] Im Gegensatz zu den übrigen virtuellen Währungen dienen *stable coins* kaum als Investitions- beziehungsweise Spekulationsobjekt.[52] Die Volatilität lässt sich auf zentralem oder auf dezentralem Weg reduzieren.

Bei mit einer staatlichen Währung hinterlegten *stable coins* überweist der Erwerber einen bestimmten Betrag in staatlicher Währung an eine zentrale Emittentin, worauf er eine identische Anzahl virtueller Währungseinheiten erhält. Beispiele hierfür sind die beiden unter anderem an den US-Dollar gebundenen und auf der Ethereum-Blockchain basierenden virtuellen Währungen *tether*[53] und *TrueUSD*[54]. Erstere wird von *Tether Limited*[55] emittiert

---

50 So betrug die Abwertung beim Bitcoin im April 2013 innerhalb von zwei Tagen 83 % und im September 2017 innerhalb von vier Tagen 40 %.

51 Vgl. <https://cryptocurrencyfacts.com/what-is-a-stable-coin>.

52 Da Wertschwankungen ein grundlegendes Problem für die Tauglichkeit einer virtuellen Währung als Zahlungsmittel und die Qualifikation als «Geld» (vgl. vorne, bei Fn. 7) darstellen, werden funktionstüchtige *stable coins* gar als der «*Holy Grail Of Cryptocurrency*» bezeichnet, vgl. SHERMAN LEE, Explaining Stable Coins, The Holy Grail Of Cryptocurrency, Forbes Online 12. März 2018, <www.forbes.com/sites/shermanlee/2018/03/12/explaining-stable-coins-the-holy-grail-of-crytpocurrency/#65e7e89f4fc6>; RACHEL WOLFSON, An Explanation For The Rise Of ‹Stable Coins› As A Low-Volatility Cryptocurrency, Forbes Online 29. März 2018, <www.forbes.com/sites/rachelwolfson/2018/03/29/an-explanation-for-the-rise-of-stable-coins-as-a-low-volatility-cryptocurrency/#55f4caad5700>.

53 Vgl. <https://tether.to>. Neben dem an den US-Dollar gekoppelten *tether* gibt es eine Variante für Euro, und es ist auch eine solche für japanische Yen angekündigt.

54 Vgl. <www.trusttoken.com/trueusd>.

und erreichte Ende April 2018 eine Marktkapitalisierung von über USD 2 Milliarden.[56] Indem die Summe eingezahlter US-Dollar der Gesamtmenge der für US-Dollar ausgegebenen *tether* entspricht, wird der Kurs des *tether* bei USD 1 gehalten.[57] Bei einer wachsenden Nachfrage nach *tether* steigt im gleichen Ausmass die Menge der eingezahlten US-Dollar, während bei der Rückgabe von Währungseinheiten die hinterlegten US-Dollar zurückübertragen werden.[58] Die Unternehmung *Tether Limited*, welche mit Bitfinex verbunden ist, wird indessen für mangelnde Transparenz kritisiert und der Manipulationen an Kryptowährungsmärkten verdächtigt.[59] Ob die Deckung in US-Dollar tatsächlich besteht, wird angezweifelt.

Da zentral herausgegebene und verwaltete *stable coins* grosses Vertrauen in die Emittentin voraussetzen, werden als Alternative *dezentrale Stabilisierungsmechanismen* entwickelt. So sind erste *stable coins* geschaffen worden, bei denen virtuelle Währungseinheiten als Sicherheit dezentral in Smart Contracts hinterlegt werden. Dieses Modell wird etwa bei der Plattform *Maker* mit der virtuellen Währung *Dai* verfolgt. Der *Dai* orientiert sich ebenfalls

---

55 Nach eigenen Angaben ist die Gesellschaft «incorporated in Hong Kong with offices in Switzerland», vgl. <https://tether.to/contact-us>. Geschäftsadressen finden sich auf der Website keine, bloss eine E-Mail-Adresse. Lediglich für schriftliche Anfragen zum Datenschutz wird eine Adresse in Taiwan genannt. Dem White Paper (S. 18) zufolge wird die Gesellschaft in Hong Kong vollumfänglich von der BVI-Gesellschaft Tether Holdings Limited gehalten. Tether Limited unterhält – wiederum gemäss White Paper (S. 18) – Konten mit zwei Banken in Taiwan. Ein Schweizer Bezug liess sich nicht verifizieren. Eine Eintragung im Handelsregister oder eine Registration als Marke bestehen in der Schweiz nicht.

56 Per 30. April 2018 belief sich die Marktkapitalisierung auf USD 2,414 Mia., <https://coinmarketcap.com>. Damit gehörte *tether* zu den 20 bedeutendsten virtuellen Währungen.

57 Bei der Stichprobe am 30. April 2018 betrug der Wert eines *tether* USD 0.992921, <https://coinmarketcap.com>.

58 Vgl. White Paper, S. 7 f. Die *tether* können vom ursprünglichen oder einem späteren Inhaber jederzeit zurückgegeben werden, worauf der entsprechende Gegenwert in US-Dollar auf das Bankkonto des Inhabers überwiesen und der Token ausser Kraft gesetzt wird.

59 Die US-amerikanische Aufsichtsbehörde Commodity Futures Trading Commission eröffnete im Dezember 2017 gegen Tether Limited und Bitfinex eine Untersuchung, vgl. MATTHEW LEISING, U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether, Bloomberg 30. Januar 2018, <www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc>.

am US-Dollar,[60] doch existiert keine zentrale Partei, welche Wertstabilisierungsmassnahmen trifft. Ein *Dai* wird durch einen als *collateralized debt position* (CDP) bezeichneten Smart Contract auf der Ethereum-Blockchain generiert. Zugriff auf *Dai* erhält, wer Ether[61] in der Höhe des Gegenwerts des Betrags der bezogenen *Dai* in US-Dollar zuzüglich einer Sicherheitsmarge *(collateral)* an den Smart Contract überträgt.[62] Der Umfang der verlangten Sicherheit beträgt derzeit 50 % der entsprechenden *Dai*.[63] Die Ether werden gesperrt und erst wieder freigegeben, wenn die vom Smart Contract emittierten *Dai* zurückübertragen werden. Steigt der Gegenwert der hinterlegten Sicherheit auf der Basis des US-Dollars, können weitere *Dai*-Währungseinheiten aus dem Smart Contract bezogen werden. Sinkt hingegen der Wert, müssen entweder gewisse *Dai* zurückbezahlt oder zusätzliche Ether als Sicherheit hinterlegt werden. Fällt das Verhältnis zwischen ausgegebenen *Dai* und hinterlegter Sicherheit unter einen bestimmten Schwellenwert *(«liquidation ratio»)*, wird der Smart Contract automatisch liquidiert und die darin hinterlegte Sicherheit in Ether gegen *Dai* veräussert. Letztere werden anschliessend zur Erhöhung des Werts der übrigen *Dai* entfernt.[64]

Überdies wird mit *stable coins* experimentiert, bei denen ein dezentrales System den Wert ohne Hinterlegung von Sicherheiten einzig durch Anpassung der Menge an Werteinheiten zu regulieren versucht.[65] Ein solches Mo-

---

60 Bei der Stichprobe am 30. April 2018 betrug der Wert eines *Dai* USD 0.996492, die gesamte Marktkapitalisierung belief sich auf USD 30,212 Mio., <https://coinmarketcap.com>.

61 In der ersten Phase des Projekts werden als Sicherheit ausschliesslich «Pooled Ether» (PETH) akzeptiert. Diese virtuelle Währung ist insofern an den Ether gebunden, als ein Smart Contract für einen Ether einen PETH generiert, doch könnte der PETH bei grossen Schwankungen abgewertet werden.

62 Vgl. White Paper vom Dezember 2017, S. 3 ff.; <https://developer.makerdao.com/dai/1>.

63 Somit werden zur Generierung von 100 *Dai* Ether im Wert von USD 150 benötigt.

64 Der Inhaber des Smart Contract erhält die einbezahlten Ether abzüglich des Werts der *Dai* sowie einer Stabilitäts- und einer Liquidationsgebühr zurück, vgl. White Paper (Fn. 62), S. 11 f.

65 Während Wertanstiege durch die Ausgabe von zusätzlichen virtuellen Währungseinheiten abgefedert werden sollen, veräussert das System im Falle von Wertverlusten in einem Token verbriefte «Seigniorage-Anteile», das heisst Rechte an den zukünftigen Erträgen bei der Schaffung neuer Werteinheiten. Diese Token sind üblicherweise vom *stable coin* unabhängig, jedoch ist der *stable coin* das einzig mögliche Zahlungsmittel. Dadurch werden Werteinheiten aus dem Verkehr gezogen, was einen Wertanstieg der virtuellen Währung bezwecken soll.

dell strebt *Basis* mit einer an den US-Dollar geknüpften virtuellen Währung an.[66] Schliesslich versuchen Projekte wie *Havven* mit der virtuellen Währung *nomin* (eUSD), das Konzept der Besicherung mit der Anpassung der Werteinheitenmenge zu kombinieren.[67]

3. Verfügung über virtuelle Währungen

Eine Verfügung über Einheiten einer Kryptowährung spielt sich, illustriert am Beispiel Bitcoin, vereinfacht wie folgt ab: Jeder Inhaber einer Währungseinheit verfügt über ein asymmetrisches, kryptografisches Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel *(public key)*, aus welchem eine Adresse[68] abgeleitet wird, und einem privaten Schlüssel *(private key)*.[69] Die verfügbaren Währungseinheiten befinden sich bei der Bitcoin-Blockchain beispielweise als sogenannte *unspent transaction outputs* (UTXO)[70] in der Blockchain-Datenbank und sind stets mit einem privaten Schlüssel verknüpft. Will der Inhaber einer Währungseinheit eine Transaktion durchführen, nimmt er den eigenen privaten Schlüssel sowie die Adresse der Empfängerin und bewirkt mit einem oder mehreren ihm zugeordneten UTXO eine Transaktion. Dabei wird ein neuer UTXO in der Höhe des Transaktionsbetrags erstellt, welcher wiederum nur mit dem privaten Schlüssel der Empfängerin weiterübertragen werden kann.[71]

---

66 Vgl. <www.basis.io>; CONNIE LOIZOS, Basis, a year-old startup that's building a price-stable cryptocurrency, just raised $ 133 million from top investors, Techcrunch 18. April 2018, <https://techcrunch.com/2018/04/18/basis-a-year-old-startup-thats-building-a-price-stable-cryptocurrency-just-raised-133-million-from-top-investors>.

67 Vgl. <https://havven.io>.

68 Die Adresse stellt ein Hash des öffentlichen Schlüssels dar und wird für die Übertragung virtueller Währungseinheiten verwendet.

69 JACQUEMART/MEYER, GesKR 2017, S. 471.

70 Vgl. <https://bitcoin.org/en/glossary/unspent-transaction-output>.

71 UTXO entstehen einerseits jeweils als Block-Entschädigung für einen Miner sowie als Resultat von Transaktionen und sind anderseits die Grundlage jeder neuen Transaktion. Sie variieren in ihrem Nennwert, wobei dieser von der kleinsten Einheit, einem Satoshi, bis zu beliebig vielen Bitcoin reicht. Für eine Transaktion über einen Bitcoin lassen sich beispielsweise drei UTXO über 0,3, 0,5 und 0,4 Bitcoin einsetzen. Da UTXO immer nur vollständig verwendet werden können, wird als Resultat dieser Transaktion ein neuer UTXO über einen Bitcoin verbunden mit dem privaten Schlüssel der Empfängerin sowie ein zweiter UTXO über 0,2 Bitcoin als «Wechselgeld» verbunden mit dem privaten Schlüssel des Senders generiert.

Andere Blockchainsysteme wie Ethereum basieren demgegenüber auf einem *Konto-Modell*, bei welchem jedem kryptografischen Schlüsselpaar ein Konto mit einem Guthaben zugeordnet ist.[72] Unabhängig von der technischen Ausgestaltung der virtuellen Währungseinheiten sind die privaten Schlüssel Dreh- und Angelpunkt solcher Überweisungen. Sie ermöglichen dem Inhaber den Zugriff auf und die Verfügung über die virtuellen Währungseinheiten.[73]

Alternativ ist denkbar, dass über virtuelle Währung verfügt wird, indem direkt der *private key* auf die Empfängerin übertragen wird. Wählen die Parteien diese Verfügungsform, setzen sie sich gewissen Risiken aus, so der Gefahr, dass der *private key* nicht Zugang zu den versprochenen virtuellen Währungseinheiten gewährt.

4. Schuld in virtueller Währung

a) Ziel

In diesem Abschnitt wird die Schuld in virtueller Währung näher untersucht. Mit Blick auf die obligationenrechtlichen Bestimmungen ist zu klären, in welchen Währungseinheiten die auf eine virtuelle Währung lautende Schuld erfüllt werden muss (I.4.b), ob eine Geldschuld im Sinne von Art. 84 Abs. 1 OR vorliegt (I.4.c), ob die virtuelle Währung als Fremdwährung qualifiziert werden kann und was in diesem Zusammenhang die Bedeutung der staatlichen Herausgabe oder Anerkennung virtueller Währungen ist (I.4.d), wie sich die Rechtslage ohne staatliche Anerkennung gestaltet (I.4.e) und ob der Leistungsumfang bei starken Wertveränderungen angepasst werden kann (I.4.f).

b) Massgebliche Währungseinheiten

Aus Art. 84 Abs. 1 OR geht hervor, dass eine Geldschuld in gesetzlichen Zahlungsmitteln der geschuldeten Währung zu bezahlen ist (vgl. vorne, bei Fn. 12). Bei staatlichen Währungen bestimmt gemäss Art. 147 Abs. 1 IPRG das öffentliche Recht des betroffenen Staates *(lex monetae)* die gesetzlichen Zahlungsmittel (vorne, bei Fn. 29). Wie noch zu erörtern ist, unterscheiden

---

72 Vgl. <https://github.com/ethereum/wiki/wiki/Design-Rationale>, Abschnitt «Accounts and not UTXOs».

73 Näher zur Funktion des *private key* bei Bitcoin JACQUEMART/MEYER, GesKR 2017, S. 471.

sich die meisten derzeit bestehenden virtuellen Währungen stark von staatlichen Währungen. Eine direkte Anwendung von Art. 84 Abs. 1 OR ist aus heutiger Sicht ausgeschlossen, weil bei privaten virtuellen Währungen keine «gesetzlichen Zahlungsmittel» existieren.

Gleichwohl ist der Grundgehalt dieser Bestimmung auch für virtuelle Währungen massgeblich: Muss ein Schuldner Einheiten einer virtuellen Währung auf eine Gläubigerin übertragen, ist die tatsächlich oder nach dem Vertrauensprinzip vereinbarte Währung geschuldet, beispielsweise Bitcoin oder Ether. Es gelten die jeweiligen Rechnungseinheiten samt Untereinheiten, bei Bitcoin etwa «Satoshi». Sollten ausnahmsweise wie bei gesetzlichen Zahlungsmitteln verschiedene Ausprägungen einer virtuellen Währung bestehen, können diese nach Wahl des Schuldners verwendet werden, sofern sie – ähnlich den Münzen und Noten der Landeswährung – allgemein akzeptiert werden. Andernfalls ist die Zustimmung der Gläubigerin erforderlich. Nach einer erfolgreich durchgeführten Spaltung einer virtuellen Währung *(hardfork)* ist grundsätzlich von zwei verschiedenen virtuellen Währungen auszugehen.[74] Eine Schuld in Bitcoin kann deshalb nicht in Bitcoin Cash erfüllt werden, sofern die Parteien dies nicht vereinbart haben. Kommt es zwischen Entstehung und Erfüllung der Schuld zu einer Spaltung der vereinbarten virtuellen Währung, ist die Rechtslage möglicherweise unklar.[75]

c) Qualifikation als Geldschuld

Regelmässig wird diskutiert, ob eine virtuelle Währung Geld und die Pflicht zur Leistung in virtueller Währung eine Geldschuld darstelle. Richtig ist, dass virtuelle Währungen typischerweise als *Zahlungsmittel* konzipiert sind.[76] Insoweit kommt ihnen Zahlungsfunktion zu und können sie – eine gewisse Verbreitung vorausgesetzt – als Geld in weiterem Sinne (vorne, bei Fn. 10) aufgefasst werden. Dazu in Kontrast steht der Umstand, dass virtuel-

74 Zum Phänomen von Hardforks vgl. JACQUEMART/MEYER, GesKR 2017, S. 473 ff.

75 Auf die *Bezeichnung* der beiden Blockchain-Stränge im Rahmen einer Spaltung lässt sich nicht ohne Weiteres abstellen. Beim Bitcoin-/Bitcoin-Cash-Hardfork erhielt der neue, angepasste Kettenstrang eine abweichende Bezeichnung (Bitcoin Cash), während beim Ethereum-/Ethereum-Classic-Hardfork der ursprüngliche, unveränderte Kettenstrang mit einem anderen Namen (Ethereum Classic) versehen wurde.

76 Nach hier vertretenem Verständnis handelt es sich bei der – zumindest theoretischen – Verwendungsmöglichkeit als Zahlungs- beziehungsweise Tauschmittel um ein begriffsnotwendiges Wesensmerkmal virtueller Währungen, vgl. vorne, bei Fn. 41.

le Währungen bislang in der Praxis nur punktuell als Zahlungsmittel eingesetzt werden.[77] Ihr Aufschwung als Anlageinstrument im Zuge der spekulativen Phase um die Jahreswende 2017/2018 ging nicht mit einer zunehmenden Verbreitung als Zahlungsmittel einher. Theoretisch betrachtet können virtuelle Währungen als abstrakte *Rechnungseinheit* (vorne, bei Fn. 7) verwendet werden. Als Massstab für die Bewertung von Gütern und Dienstleistungen eignet sich jedoch ein Betrag in einer virtuellen, nicht wertstabilisierten Währung (vgl. vorne, I.2.e.ee) wegen der zumeist hohen Volatilität kaum. Die Volatilität stellt ebenso die Tauglichkeit als *Wertaufbewahrungsmittel* in Frage.[78] Markante Kursveränderungen schliessen die Qualifikation als Zahlungsmittel oder Geld nicht zwingend aus, werfen aber die Frage auf, ob ein vereinbarter Betrag nachträglich in der Höhe angepasst werden kann (hinten, I.4.f).

Ungeachtet der obigen Ausführungen ist eine begriffliche Einstufung als Geld oder Geldschuld losgelöst von konkreten Gesetzesbestimmungen wenig sinnvoll. Überdies ist es problematisch, virtuelle Währungen als einheitliche Erscheinungsform zu behandeln, denn die Ausgestaltung und Verbreitung variieren stark. Bei *stable coins* (vorne, I.2.e.ee), welche an eine staatliche Währung gebunden sind, ist eine Qualifikation als Geld eher gerechtfertigt als bei einer virtuellen Währung ohne Bezug zu einer staatlichen Währung. Soweit die Marginalie von Art. 84 OR in Frage steht, ist schliesslich zu beachten, dass Art. 85–90 OR nach der Lehre nicht auf Geldschulden beschränkt sind.[79]

---

77 Zum Teil wird der Geldcharakter davon abhängig gemacht, dass eine virtuelle Währung eine «so hohe Akzeptanz erhält, dass sie in einem breiten Adressatenkreis als Tauschmittel eingesetzt werden kann», EGGEN, Jusletter 4. Dezember 2017, Rz. 12 m.w.H. Dieser Ansatz bedeutet, dass für jede virtuelle Währung individuell zu beurteilen ist, ob sie als Geld betrachtet werden muss, und die Qualifikation mit der zunehmenden Verbreitung einer bestimmten virtuellen Währung ändern kann.

78 Vgl. Bericht virtuelle Währungen, S. 10 (Bitcoin erscheint «eher als riskantes Spekulationsobjekt»); EZB-Stellungnahme, Ziff. 1.1.2 und 1.1.3 m.w.H. (Tausch-, nicht Zahlungsmittel, aber auch Verwendung für Wertaufbewahrungsprodukte zu Spar- und Anlagezwecken).

79 BK OR-WEBER, Art. 84 N 4.

d) Staatlich anerkannte virtuelle Währungen

aa) Bedeutung

Zahlreiche Staaten prüfen derzeit die Schaffung einer eigenen virtuellen Währung.[80] Wird eine virtuelle Währung auf gesetzlicher Grundlage von einem Staat ausgegeben oder als gesetzliches Zahlungsmittel qualifiziert, liegt es nahe, die Währungseinheiten wie eine traditionelle *Fremdwährung* zu behandeln.[81] Die rechtliche Zuordnung einer virtuellen Währung zu einem Staat ermöglicht es, dessen Vorschriften als *lex monetae* (vorne, bei Fn. 30) zu konsultieren, um die Qualifikation als Währung zu überprüfen. Teilweise wird in einem solchen Fall gar nicht von einer virtuellen Währung gesprochen (vorne, I.2.e.dd). Weniger klar ist die Situation, wenn ein Staat eine bestimmte privat herausgegebene virtuelle Währung – beziehungsweise mehrere Erscheinungsformen davon oder virtuelle Währungen generell – bloss als Zahlungsmittel anerkennt, das heisst für den Zahlungsverkehr ausdrücklich zulässt, ohne damit eine Qualifikation als *gesetzliches* Zahlungsmittel und eine Annahmeobliegenheit für Gläubigerinnen (vgl. vorne, bei Fn. 35) zu verbinden. Dass eine private virtuelle Währung im Interesse der Wertstabilisierung an eine staatliche Währung gebunden wird (vorne, I.2.e.ee), führt noch nicht zu einer staatlichen Anerkennung. Doch wird dadurch die Volatilität reduziert und so ein mögliches Hindernis für eine Qualifikation als Geld ausgeräumt.

bb) Schweiz

Keine Spielart einer virtuellen Währung ist in der Schweiz derzeit als gesetzliches Zahlungsmittel anerkannt, wie sich unzweifelhaft aus Art. 2 WZG (vgl. vorne, bei Fn. 34) ergibt. Weniger klar ist, inwieweit virtuelle Währungen gemäss einer ausländischen Rechtsordnung als Zahlungsmittel staatliche Anerkennung finden und gestützt darauf in der Schweiz als *Fremdwährungen* zu betrachten sind, was die Anwendung von Art. 84 Abs. 2 OR nahelegen würde. Im Folgenden ist für einige ausgewählte Länder zu erörtern, wie virtuelle Währungen behandelt werden beziehungsweise welche Pläne für die Schaffung einer eigenen virtuellen Währung bestehen.

---

80 Vgl. ZELLWEGER-GUTKNECHT, Jusletter 31. Oktober 2016, insbesondere N 47 ff.

81 Vgl. BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 143.

cc) Japan

In einem weltweit viel beachteten Schritt hat Japan im Frühjahr 2016 den Begriff *«virtual currency»* in Art. 2 Ziff. 5 des Payment Services Act[82] erstmalig gesetzlich definiert und Börsen für virtuelle Währungen der Finanzmarkt- und Geldwäschereiaufsicht unterstellt.[83] Die Änderung trat am 1. April 2017 in Kraft. Ausdrückliches negatives Kriterium der Definition ist, dass es sich dabei nicht um die Währung Japans oder um Fremdwährungen handelt.[84] Zu einem gesetzlichen Zahlungsmittel erhoben wurden virtuelle Währungen demnach nicht. Daraufhin publizierte Medienberichte, wonach der Bitcoin in Japan zu einer Landeswährung beziehungsweise einem gesetzlichen Zahlungsmittel *(«legal tender»)* geworden sei, sind irreführend gewesen und später zum Teil korrigiert worden.[85]

dd) Venezuela

Anders als Japan möchte die sozialistische Regierung von Venezuela im Kampf gegen die Inflation und Wirtschaftssanktionen eine eigene, auf Ethereum basierende Kryptowährung namens Petro schaffen. Dabei handelt es sich um eine staatliche Nebenwährung.[86] Die Regierung stellt in Aussicht, die Währung für Steuern und Gebühren anzunehmen. Mit Ausnahme von Staatsunternehmen besteht keine gesetzliche Pflicht, Petro als Zahlungsmittel zu akzeptieren. Die Anrechnung erfolgt zum Handelswert an bewilligten Plattformen auf der Basis der traditionellen Währung Bolívar unter

---

82 Informelle Übersetzung auf <www.japaneselawtranslation.go.jp> (Suche nach «Payment Services Act»).

83 Dazu näher NAOYA ARIYOSHI/SUSUMU TANIZAWA/HIDEKI KATAGIRI, The Essential Points Of The Amendments To The Regulation On Virtual Currency Exchange Services, mondaq 21. Januar 2017, <www.mondaq.com/x/554128/Financial+Services/The+Essential+Points+Of+The+Amendments+To+The+Regulation+On+Virtual+Currency+Exchange+Services>.

84 Die weiteren Merkmale beziehen sich auf die Möglichkeit (i) der generellen Verwendung als Entgelt für den Erwerb von Gütern oder Dienstleistungen, des Kaufs von und Verkaufs an Gegenparteien sowie der elektronischen Übertragung oder (ii) des generellen gegenseitigen Tauschs mit dem Vorgenannten sowie der elektronischen Übertragung.

85 Vgl. statt vieler das Korrigendum von Reuters vom 13. Dezember 2017 für acht veröffentlichte Beiträge unter <https://uk.reuters.com/article/idUKL3N1OD35L>.

86 Eine nähere Umschreibung findet sich im White Paper, S. 12 ff., weitere Erläuterungen insbesondere für Erwerber der Währung sind auf Spanisch verfügbar (<www.elpetro.gob.ve>).

Berücksichtigung eines Discounts und hängt vom Erdölpreis ab.[87] Die Ausgabe erfolgt nach der vom 20. Februar bis zum 19. März 2018 durchgeführten Vorverkaufsphase im Rahmen eines *Initial Coin Offering*. Total geschaffen werden sollen 100 Millionen Petro. Die angebliche Sicherung der Währung durch Rohölreserven, die sich mehrheitlich im Besitz des Staates befinden, scheint bloss wirtschaftlicher Natur zu sein und jedenfalls den Inhabern der Währung keinen Anspruch auf Öl zu verleihen. Das Unterfangen wird Medienberichten zufolge von der Opposition bekämpft und als rechtswidrig kritisiert.[88]

ee) Iran

Neben Venezuela ist auch die Zentralbank Irans bestrebt, eine von der Regierung verwaltete virtuelle Währung auszugeben.[89]

ff) Schweden

Derzeit prüft die schwedische Zentralbank die Einführung einer E-Krone *(«e-krona»).* Hintergrund ist die Tatsache, dass in Schweden die Bedeutung von Bargeld stark gesunken ist. Insoweit kann die Zentralbank den Bürgerinnen und Bürgern den vorgeschriebenen direkten Zugang zu den gesetzlichen Zahlungsmitteln – Noten und Münzen – mangels Nachfrage nicht mehr gewähren. Dadurch nimmt die Abhängigkeit von privaten Banken und ähnlichen Intermediären zu. Ein erster Zwischenbericht ist im September 2017 veröffentlicht worden.[90] Einzelheiten sind noch nicht bestimmt. Diskutiert wird technisch eine Plattform auf der Basis einer Blockchain, wobei die Wallets zwecks Verhinderung von Missbräuchen für grössere Beträ-

---

87 Die Berechnungsformel findet sich auf der erwähnten Website (Fn. 86) beziehungsweise im White Paper, S. 14.

88 Vgl. etwa PATRICIA LAYA, Venezuela Is Jumping Into the Crypto Craze, Bloomberg Businessweek 20. Februar 2018, <https://www.bloomberg.com/news/articles/2018-02-20/venezuela-is-jumping-into-the-crypto-craze>; JOHN OTIS, Venezuela's new bitcoin: an ingenious plan or worthless cryptocurrency?, The Guardian 19. Februar 2018, <www.theguardian.com/world/2018/feb/19/venezuelas-new-bitcoin-n-ingenious-plan-or-worthless-cryptocurrency>.

89 Vgl. ANNALIESE MILANO, The Next Petro? Iranian Minister Reveals Cryptocurrency Plans, CoinDesk 22. Februar 2018, <www.coindesk.com/next-petro-iranian-minister-reveals-cryptocurrency-plans>.

90 Vgl. <www.riksbank.se/en-gb/financial-stability/payments/e-krona>. Auf der Webseite findet sich auch ein Aktionsplan zum weiteren Vorgehen.

ge unter Umständen nicht pseudonym geführt werden. Das Bargeld soll erhalten bleiben, auch für Notsituationen wie Elektrizitätsausfälle. Soweit ersichtlich geht es nicht um die Schaffung einer neuen Währung, sondern bloss um eine digitale Ergänzung der bisherigen gesetzlichen Zahlungsmittel. Der Kurs der E-Krone würde der traditionellen Währung entsprechen, sodass sich das Problem der Wertschwankungen hier nicht stellt.

gg) Beurteilung

Ein Staat beziehungsweise eine Staatengemeinschaft kann virtuelle Währungen geld- und währungspolitisch auf unterschiedliche Weise berücksichtigen. Am weitesten ginge die vollständige *Ersetzung* der bisherigen Währung durch eine besondere, vom Staat ausgegebene virtuelle Währung. Für diesen im Moment unwahrscheinlichen Fall müsste aus Schweizer Sicht eine Fremdwährung bejaht werden. Demgegenüber wird in der EU die Qualifikation von virtuellen Währungen als Währungen generell abgelehnt,[91] allerdings ohne den Sonderfall der staatlichen Ausgabe besonders anzusprechen.

Gibt der Staat eine virtuelle Währung in *Ergänzung* zur bisherigen Währung heraus, geniesst sie zwar staatliche Anerkennung als Währung und gegebenenfalls als gesetzliches Zahlungsmittel, doch ist ihre Natur mit der herkömmlichen Währung nicht ohne Weiteres vergleichbar. Es liegt hier eine Währung vor, deren Merkmale gestützt auf Art. 147 Abs. 1 IPRG (vorne, bei Fn. 30) anhand der ausländischen Gesetzgebung zu spezifizieren sind. Zentral ist jeweils die Frage, ob es sich bei der virtuellen Währung um eine selbstständige Zweitwährung handelt oder lediglich um eine digitale Form derselben Währung in Ergänzung von Noten, Münzen und herkömmlichem elektronischen Geld, ähnlich wie es die schwedische Zentralbank anvisiert (vorne, bei Fn. 90). Ob die Währung durch den Besitz einer Münze, eine Gutschrift auf einem Bankkonto oder Einheiten der staatlichen virtuellen Währung repräsentiert wird, ist für die zivilrechtliche Beurteilung zumeist nicht entscheidend. Doch ist etwa zu klären, ob eine Gläubigerin die Obliegenheit trifft, die Erfüllung einer Forderung durch Übertragung virtueller Währungseinheiten zu akzeptieren, um nicht in Annahmeverzug zu geraten (vorne, bei Fn. 14).

Wie das Beispiel Japan zeigt, rechtfertigt die blosse *Anerkennung* einer bestimmten privaten virtuellen Währung oder von virtuellen Währungen

[91] Vgl. EZB-Stellungnahme, Ziff. 1.1.3 m.w.H.

generell durch einen beliebigen ausländischen Staat nicht unbesehen deren zivilrechtliche Qualifikation als Fremdwährung aus Sicht der Schweiz. In einem solchen Fall wird die staatliche Währung weiterhin existieren. Auch ist denkbar, dass mehrere Staaten ein und dieselbe virtuelle Währung anerkennen, sodass die Währung durch mehrere Rechtsordnungen geregelt wird. Womöglich betrifft die Anerkennung indessen gar nicht den Status als gesetzliches, sondern bloss als privates Zahlungsmittel und bedeutet lediglich, dass der Staat dessen Verwendung nicht verbietet. Häufig geht es darum, die Unterstellung unter die Geldwäschereivorschriften sicherzustellen. Eine generelle Aussage, wie sich die Anerkennung durch einen ausländischen Staat auf die zivilrechtliche Qualifikation in der Schweiz auswirkt, ist nicht möglich.

Von der Anerkennung durch einen Staat zu unterscheiden ist der Fall, dass eine private virtuelle Währung zwecks Wertstabilisierung an eine staatliche Währung *geknüpft* wird (vorne, I.2.e.ee). Dieser Umstand ist für die zivilrechtliche Qualifikation bloss insoweit relevant, als dadurch die Volatilität reduziert wird.

e) Virtuelle Währungen ohne staatliche Anerkennung

Fehlt es an einer staatlichen Ausgabe oder Anerkennung, lassen sich die Merkmale einer virtuellen Währung nicht anhand eines gesetzlichen Währungsstatuts im Sinne von Art. 147 Abs. 1 IPRG bestimmen. Die Eigenschaften der virtuellen Währung hängen von der technischen Ausgestaltung der Währung ab. Dabei sind auch bei einem dezentralen virtuellen Währungssystem Änderungen an den zugrunde liegenden Parametern denkbar, sofern diese durch die erforderliche Mehrheit des *Peer-to-Peer*-Netzwerks mitgetragen werden.

Für die rechtlichen Modalitäten der Erfüllung gilt grundsätzlich das *Schuldstatut* (vorne, bei Fn. 20). Untersteht die Schuld Schweizer Recht, ist diese in analoger Anwendung von Art. 84 Abs. 1 OR in der vereinbarten virtuellen Währung zu erfüllen. Die Leistung in einer anderen Währung als der vorgesehenen ist unter Umständen aus technischen Gründen gar nicht möglich. Auch wenn bei virtuellen Währungen nicht eine klassische Geldschuld vorliegt, erscheinen die Anwendung des Nennwertprinzips (vorne, bei Fn. 18) und der Ausschluss der subjektiven Unmöglichkeit (vorne, bei Fn. 24) sinnvoll. Infolgedessen bleibt trotz der typischerweise hohen Volatilität virtueller Währungen der Betrag im Zeitpunkt der Entstehung der Schuld massgeblich. Ob in Fällen extremer Wertschwankungen von diesem

Grundsatz abgewichen werden kann, ist im Folgenden anhand der früheren Rechtsprechung des schweizerischen Bundesgerichts zur deutschen Mark zu überprüfen.

f) Nachträgliche Wertanpassungen

In einer Reihe von Urteilen aus den 1920er- und 1930er-Jahren ist das Bundesgericht der Frage nachgegangen, wann es sich rechtfertigt, das Nennwertprinzip wegen Wertschwankungen der vereinbarten Währung zu durchbrechen. In diesen Fällen ging es um die «Mark deutscher Währung», welche nach dem Ersten Weltkrieg einen nahezu vollständigen Wertzerfall erlitt: Das deutsche Münzgesetz vom 30. August 1924 führte als neue Währung die Reichsmark ein und setzte eine Billion Mark der bisherigen Währung (Papiermark) einer Reichsmark gleich. Dadurch wäre bei einem Darlehen «*die Rückzahlung in Papiermark einer vollständigen Auslöschung der Schuld*» gleichgekommen[92] oder bei zwei Leibrentenverträgen die geschuldete Leistung von jährlich je 400 Papiermark so gering gewesen, dass «*zur Zeit des Abschlusses der Verträge gar kein Geldzeichen bestand, durch dessen Hingabe sie hätte entrichtet werden können*».[93] Das Bundesgericht befürwortete deshalb umfangreiche Aufwertungen der geschuldeten Beträge.[94] Der Zeitraum seit dem Vertragsschluss betrug jeweils mehrere Jahre. Begründet wurden die gerichtlichen Aufwertungen nicht mit der *clausula rebus sic stantibus* (vgl. vorne, bei Fn. 23), sondern mit der damaligen Gesetzgebung und Rechtsprechung in Deutschland, welche derartige Aufwertungen ausdrücklich anordnete, aufgrund der besonderen Umstände indessen nicht direkt Anwendung fand, sowie mit Treu und Glauben beziehungsweise einer entsprechenden Vertragsauslegung oder Vertragslücke.

Folglich ist gemäss Rechtsprechung das im Nennwertprinzip verkörperte Vertrauen in die Stabilität einer Währung in Ausnahmefällen nicht mehr

---

92 BGE 51 II 303 E. 3 S. 307.

93 BGE 53 II 76 E. 3 S. 79. In Deutschland regelte das Aufwertungsgesetz vom 16. Juli 1925 die Aufwertung von Versicherungsansprüchen.

94 Vgl. BGE 57 II 368 E. 4 S. 371 f. (Aufwertung einer Versicherungssumme auf 34 % des Goldmarkwerts der Versicherung); BGE 53 II 76 E. 3 S. 84 (Aufwertung der unter den beiden Verträgen geschuldeten Leibrenten von jährlich je 400 Papiermark auf 70 % der Beträge in Reichsmark); BGE 51 II 303 E. 5 S. 313 (Aufwertung einer Darlehensforderung von 8000 Mark auf 2400 [= 30 %] Goldmark).

schützenswert.[95] In den erwähnten Urteilen ging es um die Inflation, doch ist anzunehmen, dass ähnliche Kriterien für markante Kurssteigerungen herangezogen werden können. Unabhängig davon, ob die gerichtliche Anpassung auf die *clausula rebus sic stantibus*, Treu und Glauben oder eine Vertragsauslegung gestützt wird, ist vorauszusetzen, dass die Wertveränderung für die Parteien im Zeitpunkt des Vertragsschlusses nicht vorhergesehen werden konnte.[96] Dieses Erfordernis wird durch die erwähnte Gerichtspraxis bestätigt: Zwar wird erwähnt, dass eine Vertragspartei die Gefahr einer Währungsentwertung in gewissem Umfang zu tragen habe, vorliegend die Papiermark bereits im Zeitpunkt der Vereinbarung erheblich entwertet und eine zusätzliche Verminderung der Kaufkraft nicht ausgeschlossen gewesen sei. Doch musste nur mit teils natürlichen, teils zufälligen Schwankungen gerechnet werden, während eine völlige Entwertung nicht voraussehbar war und von niemandem bedacht wurde.[97]

Im Gegensatz dazu sind bei den meisten virtuellen Währungen auch äusserst kurzfristige Wertveränderungen an der Tagesordnung. Es ist deshalb kaum denkbar, dass sich hier gestützt auf die genannten Grundsätze eine Abweichung vom Nennwertprinzip und eine Anpassung des Betrags der Schuld beziehungsweise der Forderung begründen lässt. Gegenteiliges gilt für *stable coins* (vorne, I.2.e.ee), bei denen die Nutzer auf die Wertstabilität vertrauen.

g) Folgerungen

Virtuelle Währungen sind typischerweise für den Einsatz als Zahlungsmittel konzipiert. Obwohl die Volatilität die Tauglichkeit als Massstab für die Bewertung von Gütern und Dienstleistungen sowie als Wertaufbewahrungsmittel beeinträchtigt (vorne, bei Fn. 78), ist es gerechtfertigt, die Qualifikation als *Geld in weiterem Sinne* und als *Zahlungsmittel* zu bejahen. Allerdings ist rechtlich damit nicht viel gewonnen: Ob die obligationenrechtlichen Bestimmungen zur Zahlung im Sinne der Marginalie von Art. 84 OR beziehungsweise zur Geldschuld anwendbar sind und virtuelle Währungen privatrechtlich wie Fremdwährungen behandelt werden dürfen, ist für die

---

95 Vgl. BGE 51 II 303 E. 4 S. 310, wonach «*der Vertrag auf das Vertrauen gegründet [war], dass der Mark innerhalb gewisser Grenzen Wertbeständigkeit zukommen werde*».

96 Zur *clausula rebus sic stantibus* BGE 127 III 300 E. 5b S. 305 (Verhältnisänderung weder vorhersehbar noch vermeidbar).

97 BGE 51 II 303 E. 4 S. 309 f.

massgeblichen Vorschriften je separat zu prüfen. Eine einheitliche Qualifikation der virtuellen Währungen für das gesamte Zivilrecht ist nicht möglich. Auch können je nach virtueller Währung Differenzierungen erforderlich sein.

Im Grundsatz ergibt sich, dass eine *generelle* direkte Anwendung der obligationenrechtlichen Bestimmungen zu Geld- oder Fremdwährungsschulden abzulehnen ist, da sich virtuelle Währungen grösstenteils stark vom herkömmlichen Geld unterscheiden. Wegen der funktionellen Verwandtschaft sind punktuell Anleihen bei Zahlungen in traditionellem Geld gerechtfertigt. Die Schuld ist grundsätzlich in der vereinbarten virtuellen Währung zu erfüllen. Auch gilt das *Nennwertprinzip.* Abweichungen davon sind kaum denkbar, weil die exzessiven Wertveränderungen bei den meisten virtuellen Währungen mit Ausnahme von *stable coins* allgemein bekannt und deshalb voraussehbar sind.

Eine Geld- beziehungsweise Fremdwährungsschuld wäre zu bejahen, falls ein ausländischer Staat seine bisherige Währung vollständig durch eine von ihm neu ausgegebene virtuelle Währung ersetzen oder die bisherigen gesetzlichen Zahlungsmittel um eine gleichberechtigte digitale Spielart in derselben Währung ergänzen würde. Bei einer blossen Anerkennung durch einen ausländischen Staat als zulässiges Zahlungsmittel ohne Annahmeobliegenheit für Gläubigerinnen muss im Einzelfall geprüft werden, welche zivilrechtlichen Folgen daraus abgeleitet werden können. Weist eine private virtuelle Währung aufgrund ihrer Anbindung an eine staatliche Währung ähnliche Eigenschaften wie die staatliche Währung auf, kann eine analoge Anwendung von Bestimmungen über Fremdwährungen gerechtfertigt sein.

5. Modalitäten der Erfüllung

a) Leistung in Drittwährung

aa) Staatliche Währungen[98]

Zu untersuchen ist, ob der Schuldner seine Schuld statt in der vereinbarten virtuellen Währung in einer anderen virtuellen beziehungsweise einer staatlichen Währung oder statt in der vereinbarten staatlichen in einer virtuellen

[98] Unter «staatlicher» Währung wird hier in der Regel eine traditionelle «Landeswährung» im Sinne von Art. 84 Abs. 2 OR verstanden, unter Ausklammerung der Möglichkeit, dass die staatliche Währung ihrerseits virtueller Natur sein könnte (vorne, I.2.e.dd).

Währung begleichen darf und wie der Umrechnungskurs zu bestimmen ist. Gemäss Art. 147 Abs. 3 IPRG ist für die Bestimmung der Währung wie erwähnt (vorne, bei Fn. 33) auf die Rechtsordnung am vertraglich oder gesetzlich vorgesehenen Zahlungsort abzustellen. Liegt dieser auch tatsächlich in der Schweiz,[99] darf eine Schuld in Fremdwährung nach Art. 84 Abs. 2 OR mangels Effektivklausel in der schweizerischen Landeswährung beglichen werden. Das Wahlrecht kommt dem Schuldner zu. Das Obligationenrecht sieht die Umrechnung zum Zeitpunkt der Fälligkeit vor. Im Übrigen bestimmt sich die Umrechnung nach dem auf die Schuld anwendbaren Recht. Bei einem Zahlungsort im Ausland könnte die Schuld in der anerkannten lokalen Währung erfüllt werden, doch wird Art. 84 Abs. 2 OR aufgrund von Art. 147 Abs. 3 IPRG nicht anwendbar sein. Vorauszusetzen ist stets, dass eine Währung geschuldet ist, welche am Zahlungsort nicht Landeswährung ist, das heisst nicht dortigen gesetzlichen Zahlungsmitteln entspricht.[100]

Ausserhalb des Anwendungsbereichs von Art. 84 Abs. 2 OR kann die Gläubigerin den Schuldner ermächtigen, die in einer bestimmten Währung geschuldete Leistung in einer anderen Währung zu erfüllen *(Alternativermächtigung).* Geschuldet ist nur die Leistung in der vereinbarten Währung. An Erfüllungs statt (sogleich hinten, bei Fn. 101) darf der Schuldner die geschuldete Hauptleistung durch Erbringung einer anderen Leistung erfüllen.

Demgegenüber sind bei einer *Währungsoptions-* oder *Alternativwährungsklausel* alternativ zwei oder mehr Währungen geschuldet, wobei oft die Gläubigerin die massgebliche Währung wählen kann. Fehlt es an einer Vereinbarung, steht bei der Wahlobligation nach Art. 72 OR die Wahl dem Schuldner zu. Die ausgewählte Leistung wird ursprünglich geschuldet.

bb) WIR

In BGE 119 II 227 vereinbarten die Parteien eines Kaufvertrags die Bezahlung des Preises von CHF 19'542.- in «100 % WIR», ohne Teilnehmer des WIR-Netzwerks zu sein. Als die WIR Bank Genossenschaft die Ausführung der von der Käuferin vorgelegten WIR-Buchungsaufträge wegen Verletzung der Geschäftsbedingungen verweigerte, verlangte die Verkäuferin nach erfolgloser Mahnung die Zahlung des Kaufpreises in Franken. Gemäss Bundesgericht ist im Zweifelsfall eine *Leistung erfüllungs-* oder *zahlungshalber*,

[99] Art. 84 Abs. 2 OR stellt auf den effektiven Zahlungsort ab.

[100] Vgl. ZK OR-SCHRANER, Art. 84 N 175 m.w.H.

nicht eine solche an Erfüllungs oder Zahlungs statt,[101] zu vermuten.[102] Dadurch wird die Gläubigerin geschützt, welche akzeptiert, vom Schuldner eine andere Form als eine Geldleistung anzunehmen. Die erfüllungshalber erbrachte Leistung wird angerechnet, sie ersetzt aber die ursprünglich geschuldete Leistung nicht. Letztere wird bis zur vollständigen Erfüllung gestundet. Der Schuldner wird somit nicht befreit. Nach dem Bundesgericht entsteht mit der Hingabe der Leistung erfüllungshalber zwischen der Gläubigerin und dem Schuldner ein *auftragsähnliches Rechtsverhältnis*, welches die Gläubigerin verpflichtet, sich sorgfältig um die Verwertung der Ersatzleistung zu bemühen.[103] Der Verkäuferin war keine mangelnde Sorgfalt vorzuwerfen. Sie durfte deshalb von der Käuferin die Zahlung des Kaufpreises in Franken verlangen. Vorauszusetzen ist somit in solchen Fällen, dass das vertraglich vorgesehene Zahlungsmittel nicht zur Tilgung der Schuld führt und der Gläubigerin diesbezüglich keine mangelnde Sorgfalt vorzuwerfen ist.[104]

Der Einsatz der Komplementärwährung WIR zeichnet sich dadurch aus, dass als Entgelt für ein Waren- oder Dienstleistungsgeschäft ein Betrag in Franken/WIR[105] festgesetzt wird[106] und die Anbieterin anerkennt, als Erfüllungssurrogat einen bestimmten Anteil des Preises beziehungsweise Auftragswerts in WIR – beispielsweise 25 % oder 100 % WIR – zu akzeptieren.[107] Im Rahmen des veröffentlichten WIR-Annahmesatzes[108] ist die Anbieterin zur Annahme von WIR verpflichtet.[109] Die Anbieterin kann vom Abnehmer

---

101 Eine Leistung *an Erfüllungs statt* wird etwa angenommen, wenn der Schuldner eine Geldschuld durch Überweisung des Betrags auf das Bankkonto der Gläubigerin erfüllt. Die Gläubigerin erhält dadurch rechtlich betrachtet kein Geld, sondern lediglich eine Forderung gegenüber der Bank. Die Ersatzleistung tritt an die Stelle der geschuldeten Leistung.

102 BGE 119 II 227 E. 2a S. 230.

103 BGE 119 II 227 E. 3a S. 231 m.w.H.

104 BGE 119 II 227 E. 3a S. 231 f.

105 Das offizielle Kürzel für WIR lautet CHW. Zum besseren Verständnis wird vorliegend die Abkürzung WIR verwendet.

106 Die Teilnahmebedingungen schreiben vor, dass derselbe Preis Anwendung findet, unabhängig davon, ob der Kunde selbst WIR-Teilnehmer ist beziehungsweise ob er in Franken oder WIR bezahlt («Prinzip der Preisparität»).

107 Der WIR-Annahmesatz beträgt zwischen 3 % und 100 %. Die WIR Bank Genossenschaft empfiehlt branchenabhängig Mindest- und Höchstsätze.

108 Es ist möglich, je nach Geschäftsbereich, Produktkategorie oder Dienstleistung bis zu drei verschiedene WIR-Annahmesätze festzulegen.

109 Pro Geschäftsabschluss ist der WIR-Anteil an sich auf WIR 5'000 beschränkt, doch dürfen WIR-Teilnehmer individuell höhere WIR-Beträge vereinbaren.

weiterhin die Leistung in Franken verlangen, allerdings bloss subsidiär, wenn die Erfüllung in WIR fehlgeschlagen ist oder der Abnehmer in Verzug gerät (dazu hinten, bei Fn. 163). Andernfalls muss die Anbieterin das dem Abnehmer eingeräumte Recht respektieren, in WIR zu leisten.[110] Auch gegenüber der Bank haben Kunden und WIR-Teilnehmer kein Recht, die Erfüllung einer Schuld in WIR durch Leistung in Franken zu verlangen. Dies ergibt sich ausdrücklich aus den Geschäftsbedingungen.[111]

Für den Abnehmer ist es grundsätzlich vorteilhaft, in WIR bezahlen zu dürfen. Es steht ihm jedoch frei, die Leistung in Franken zu erbringen, falls er mit der Anbieterin nichts Gegenteiliges vereinbart hat. Da WIR nicht der Charakter einer staatlichen Währung zukommt (vorne, Fn. 32), ist Art. 84 Abs. 2 OR nicht anwendbar. Hätten die Parteien nicht vertraglich eine auf Franken lautende Schuld begründet, wäre der Abnehmer nicht berechtigt, statt in WIR in Franken zu leisten. Für die Anbieterin ist die Leistung in Franken nicht nachteilig, da WIR weniger liquide ist.[112]

cc) Virtuelle Währungen

Wird eine Leistung in *virtueller Währung* vereinbart, ohne den Schuldner oder die Gläubigerin zur Leistung in staatlicher Währung zu berechtigen, ist die Leistung grundsätzlich in der virtuellen Währung zu erbringen. Eine analoge Anwendung von Art. 84 Abs. 2 OR ist im Regelfall nicht gerechtfertigt. Vielmehr ist mangels gegenteiliger Abrede die Vereinbarung der *effektiven* Leistung in virtueller Währung zu vermuten. Diese Einschätzung berücksichtigt die erheblichen Unterschiede zwischen den derzeitigen virtuellen und staatlichen Währungen, insbesondere die erheblichen Wertschwankungen, die begrenzten Einsatzmöglichkeiten virtueller Währungen und die eingeschränkte Konvertierbarkeit.[113] Werden virtuelle Währungen zu Anlagezwecken erworben, versteht sich von selbst, dass der Investor die

---

110 Privatpersonen können nur in WIR bezahlen, falls ihr Arbeitgeber WIR-Teilnehmer ist. Sie benötigen hierfür ein besonderes WIR-Konto.

111 Gemäss Ziff. B.18 Abs. 1 AGB WIR (Fn. 32) hat der Kunde keinen Anspruch auf Auszahlung seines Guthabens – egal welcher Währung – in Bargeld durch die Bank. Ebenso hat der WIR-Teilnehmer keinen Anspruch auf Auszahlung von WIR in Franken oder anderer Währung durch die Bank (Ziff. C.2 Abs. 3 AGB WIR; Ziff. 2 Abs. 3 Teilnahmebedingungen WIR [Fn. 32]).

112 WIR-Teilnehmer dürfen WIR nicht zum Kauf oder Verkauf in Franken erwerben oder anbieten, sondern lediglich als Entgelt für Waren und Dienstleistungen einsetzen.

113 BÄRTSCHI/MEISSER, Virtuelle Währungen, S. 147.

virtuellen Währungseinheiten und nicht Landeswährung erlangen will. Analoges gilt beim Wechsel von virtuellen Währungen über Plattformen.

Anders zu beurteilen ist die Situation in der Regel, wenn *stable coin*s (vorne, I.2.e.ee) geschuldet sind, deren Wert an eine staatliche Währung gebunden ist. In diesem Fall handelt es sich bei der virtuellen Währung um ein nicht staatlich anerkanntes digitales «Faksimile» der Währung eines ausländischen Staates, welches teilweise ähnliche Merkmale aufweist wie die entsprechende Fremdwährung. Die Wertdifferenz gegenüber der zugrunde liegenden Fremdwährung sollte marginal sein, die Volatilität somit kaum grösser als diejenige der Fremdwährung. Eine analoge Anwendung von Art. 84 Abs. 2 OR erscheint hier vertretbar.[114] Aufgrund der eingeschränkten Konvertier- und Nutzbarkeit solcher virtuellen Währungen im Vergleich zu verbreiteten Fremdwährungen dürfte die Gläubigerin regelmässig keinen Nachteil erleiden, wenn der Schuldner die Leistung in Franken erbringt.[115] Wie bei traditionellen Fremdwährungen ist jedoch von einer effektiven Leistungspflicht auszugehen, wenn eine solche von den Parteien explizit oder konkludent vereinbart worden ist.

Wird eine *staatliche Währung* geschuldet, könnte der Schuldner gestützt auf Art. 84 Abs. 2 OR in virtueller Währung erfüllen, falls Letztere den Status als lokales gesetzliches Zahlungsmittel geniessen würde. Ein analoges Wahlrecht steht dem Schuldner zu, wenn zwei Parteien vereinbaren, dass eine auf die staatliche Währung lautende Schuld auch in virtueller Währung erfüllt werden darf. Es handelt sich in der Regel um eine blosse Erfüllungsmodalität, welche keinen Einfluss auf die Qualifikation der ursprünglichen Schuld hat.[116] Eine solche Abrede ergibt sich häufig stillschweigend, so wenn ein Anbieter von Waren oder Dienstleistungen – oftmals aus Marketingüberlegungen – ausdrücklich oder konkludent zum Ausdruck gibt, «auch»

---

114 Die lokale Landeswährung muss dabei nicht der zugrunde liegenden Fremdwährung der *stable coins* entsprechen, das heisst bei *stable coins* auf US-Dollar ist die Leistung in Franken als Landeswährung am Zahlungsort zulässig. Erst recht darf der Schuldner bei *stable coins* auf Franken direkt in Franken leisten, wenn der Zahlungsort in der Schweiz liegt.

115 Dies gilt umso mehr, wenn wie bei *tether* anlässlich der Rückgabe an die Emittentin und der Banküberweisung eine Gebühr in der Fremdwährung belastet wird, vgl. <https://tether.to/fees>.

116 Vgl. EGGEN, Jusletter 4. Dezember 2017, Rz. 18; für traditionelles Geld BK OR-WEBER, Art. 84 N 141 (uneigentliche Geldsortenschuld).

gewisse virtuelle Währungen zu akzeptieren.[117] Hierfür genügt, dass in einem Ladenlokal oder auf der Website ein entsprechendes Logo, etwa das Bitcoin-Symbol, abgebildet ist. Es ist nicht angezeigt, das Wahlrecht des Schuldners auf die dispositive Bestimmung von Art. 84 Abs. 2 OR abzustützen.

Häufig wird der Anbieter die erworbenen virtuellen Währungen zeitnah in die Landeswährung wechseln. Für den *Umrechnungskurs* bedeutet dies, dass die Gläubigerin bei einem sofortigen Umtausch in die staatliche Währung keinen Nachteil erleiden sollte. Bei Art. 84 Abs. 2 OR wird auf den Briefkurs (Angebotskurs) der Fremdwährung am Zahlungsort im Zeitpunkt der Fälligkeit abgestellt.[118] Vorliegend rechtfertigt sich angesichts der hohen Volatilität die Vermutung, dass die Parteien den Kurs im *Zeitpunkt der Leistung* (Zahlung) als massgeblich betrachten wollten. Wäre die Zeit der Fälligkeit entscheidend, müsste die Gläubigerin Kursverluste bis zur Leistung beziehungsweise spätestens bis zur Inverzugsetzung tragen; befindet sich der Schuldner im Verzug, haftet er für Kursschwankungen als «Zufall» im Sinne von Art. 103 Abs. 1 OR.[119] Bis zur Erbringung der Leistung kann der Schuldner auf einen Kursanstieg der virtuellen Währung spekulieren, sodass er für den in staatlicher Währung festgesetzten Betrag weniger virtuelle Währungseinheiten aufbringen muss. Für den Umrechnungskurs sollte – mangels Anbindung an eine staatliche Währung – auf mehrere liquide Plattformen für die entsprechende virtuelle Währung abgestellt und daraus ein Durchschnittskurs gebildet werden. Darauf ist im Zusammenhang mit der Verrechnung von virtuellen Währungen zurückzukommen (hinten, II.2). Für

---

117 Beispielsweise führte die Bergbahngesellschaft Engadin St. Moritz Mountains AG die Möglichkeit der Bezahlung von Skitickets in Bitcoin ein, vgl. Webshop, <www.mountains.ch/de/webshop>. Für eine Übersicht über Geschäfte, welche virtuelle Währungen annehmen, vgl. BTC-ECHO GmbH, Bitcoin-Akzeptanzstellen, <www.btc-echo.de/tutorial/bitcoin-akzeptanzstellen>.

118 ZK OR-SCHRANER, Art. 84 N 193 ff.; BK OR-WEBER, Art. 84 N 329 ff. Welcher Kurs heranzuziehen ist, wird in der Lehre kontrovers diskutiert; zur Massgeblichkeit des Devisen- oder Notenkurses vgl. die Hinweise bei ZK OR-SCHRANER, Art. 84 N 195 f.; BK OR-WEBER, Art. 84 N 335.

119 Bei virtuellen Währungen ist es wegen der hohen Tagesvolatilität überdies bedeutend, dass der massgebliche Zeitpunkt nicht nur – wie üblicherweise bei der Fälligkeit – nach dem Kalendertag bestimmt ist, sondern dass auch ein exakter Augenblick – wie derjenige der Zahlung – fixiert wird. Aus praktischen Gründen wird der Moment massgeblich sein müssen, in welchem der Übertragungsvorgang durch den Schuldner ausgelöst wird.

die Praxis empfiehlt sich hinsichtlich der angesprochenen Punkte eine ausdrückliche Regelung.

b) Zeitpunkt der Erfüllung

aa) Bedeutung

Wird eine Schuld in virtueller Währung beglichen, stellt sich die Frage, in welchem Zeitpunkt die Schuld als erfüllt gilt. Aus rechtlicher Sicht besteht ein Bedürfnis, einen exakten Stichzeitpunkt für die Erfüllung zu bestimmen. Dieser ist massgeblich dafür, wann die Forderung der Gläubigerin erlischt und der Schuldner als befreit gilt, er somit nicht mehr die Gefahr des zufälligen Untergangs der übertragenen Währungseinheiten trägt. Bei bargeldlosen Zahlungen hält das Bundesgericht für massgeblich, wann der Betrag auf dem Bankkonto der Gläubigerin gutgeschrieben ist, sodass diese darüber verfügen kann.[120] Wegen des abweichenden Übertragungsvorgangs (vorne, I.3) lässt sich diese Rechtsprechung nicht direkt auf virtuelle Währungen wie Bitcoin anwenden.[121] Ausschlaggebend sein darf weder der Zeitpunkt des Erscheinens im Wallet der Empfängerin noch derjenige des Auslösens der Transaktion durch den Schuldner.[122] Der Abschluss des Übertragungsvorgangs durch den Schuldner kann aus praktischen Gründen etwa massgeblich sein, um den Erfüllungsort anhand des Sitzes der Gläubigerin zu bestimmen oder für die Zwecke von Art. 82 OR die veranlasste Erfüllung zu belegen. Bei Bitcoin geht es um die UTXO-Generierung in der Höhe des geschuldeten Betrags mittels des privaten Schlüssels (vgl. vorne, bei Fn. 71). Damit wird der Vorgang der Erfüllung allerdings erst begonnen, nicht abgeschlossen. Folglich ist zu klären, wann die Schuld in virtueller Währung erfüllt und der Schuldner befreit ist.

bb) Unwiderruflichkeit einer Transaktion

Grundsätzlich hat die Gläubigerin ein legitimes Interesse daran, endgültig über die geschuldeten virtuellen Währungseinheiten verfügen zu können.

---

120 BGE 124 III 112 E. 2a S. 117 m.w.H. Der Zeitpunkt muss nicht mit dem Valutadatum übereinstimmen, welches primär für den Zinsenlauf relevant ist.

121 Die Werteinheiten existieren hier als Transaktionsoutputs auf der Blockchain verteilt. Mittels des relevanten privaten Schlüssels lassen sich diese als Inputs für neue Transaktionen verwenden (vorne, Fn. 71).

122 Gl.M. EGGEN, Jusletter 4. Dezember 2017, Rz. 29.

Das in der Lehre[123] vorgeschlagene Abstellen auf den Zeitpunkt des mutmasslich definitiven, unwiderruflichen Eintrags in das dezentrale Register bedarf einer näheren Erörterung. Der Block, auf welchem eine Transaktion gespeichert wird, ist bei einer Gabelung der Blockchain[124] zwar noch auf dieser vorhanden, wird unter Umständen aber von der Mehrheit der Netzwerkteilnehmer nicht mehr akzeptiert. Dies ist etwa der Fall, wenn sich eine konkurrierende Version der Blockchain schneller als die angestammte Fassung im Netzwerk verbreitet oder wenn eine Mehrheit der Teilnehmer gewisse Transaktionen im Rahmen einer Protokolländerung, wie beim Ether-/Ether-Classic-*Hardfork*, bewusst rückgängig machen will. Eine eigentliche Unwiderruflichkeit beziehungsweise die Sicherheit, dass das Netzwerk einen Eintrag auch in Zukunft als gültig anerkennt, ist bei einer Blockchain-Anwendung nie in absoluter Form vorhanden.[125]

cc) Hohe Wahrscheinlichkeit

Soweit es um die Bestätigung von Transaktionen und das Risiko einer anderweitigen Verfügung über die virtuelle Währung *(double spending)* geht, wird in der Praxis auf den Zeitpunkt abgestellt, in welchem der einer Transaktion zugrunde liegende Block vom Netzwerk mit hoher Wahrscheinlichkeit als gültig erachtet wird. Diese Beurteilung muss für jede virtuelle Währung individuell vorgenommen werden und hängt bei zahlreichen Systemen unter anderem von der Verteilung der Rechenleistung im Netzwerk *(hashrate)* ab. Gewisse Mining-Pools vereinigen einen beträchtlichen Anteil der Rechenleistung. Bei der Bitcoin-Blockchain kann mit der Erstellung von rund sechs folgenden Blöcken, also nach durchschnittlich einer Stunde, der Bestand einer Transaktion angenommen werden.[126] Sollte eine Gruppe von Nutzern, welche gemeinsam 10 % der Rechenleistung kontrollieren, versuchen, die Transaktion rückgängig zu machen, liegt die Erfolgschance und somit das Risiko einer späteren Ablehnung der Transaktion

123 EGGEN, Jusletter 4. Dezember 2017, Rz. 29 und 32 («sobald die Überweisung […] unwiderruflich im dezentralen Register festgehalten worden ist»).

124 Näher zu den einzelnen Arten von Blockchain-Gabelungen JACQUEMART/MEYER, GesKR 2017, S. 471 ff.

125 Vgl. zu den gängigsten Angriffsszenarien bei der Bitcoin-Blockchain (Transaction-Malleability, Double-Spending-Attacken und sonstige Angriffe) PESCH, Cryptocoin-Schulden, S. 32 ff.

126 Vgl. bitcoinwiki, Confirmation, <https://en.bitcoin.it/wiki/Confirmation>.

nach sechs Blöcken theoretisch bei unter 0,1 %.[127] Bei 40 % Rechenkapazität würde dieses Risiko rund 50 % betragen; 60 Blöcke wären nötig, damit dieses auf unter 1 % sinken würde. Zwar steigt die Schwierigkeit einer späteren Rückgängigmachung der Transaktion mit dem Anhängen weiterer Blöcke exponentiell an. Nutzer mit einer Mehrheit der Rechenkapazität könnten aber jede durchgeführte, auch weit zurückliegende Transaktion nachträglich annullieren. Die theoretisch wünschenswerte Schwelle der endgültigen Verfügungsmöglichkeit der Gläubigerin wird im Prinzip nie erreicht.[128]

Den Erfüllungszeitpunkt übermässig zu verzögern, vermag nicht zu befriedigen. Die Gefahr von Manipulationen oder nachträglichen Annullationen soll nicht dauerhaft vom Schuldner getragen werden müssen, sofern er seinerseits alle Vorkehrungen für die Übertragung der virtuellen Währungseinheiten getroffen hat. Der Schuldner kann in der Regel so wenig wie die Gläubigerin die Fortentwicklung der Blockchain steuern. Akzeptiert eine Gläubigerin die Erfüllung einer Geldschuld mittels Überweisung auf ihr Bankkonto, trägt sie ebenfalls ein Risiko, nämlich dass ihre Bank in Konkurs fällt und ihr dadurch die Verfügungsmöglichkeit über den gutgeschriebenen Betrag entzogen wird. Die Verwendung der virtuellen Währung wird von den Parteien grundsätzlich beidseitig vereinbart; ob der Schuldner oder die Gläubigerin ein besonderes Interesse daran hat, lässt sich kaum generell sagen. Ein angemessener Ausgleich besteht darin, dass der Schuldner ohne anderslautende Parteivereinbarung so lange gebunden und zur Leistung verpflichtet bleiben soll, bis die Gläubigerin die endgültige Verfügungsmöglichkeit über die transferierten virtuellen Währungseinheiten mit *sehr hoher Wahrscheinlichkeit* erlangt. Die Schuld ist mit anderen Worten erfüllt, wenn der Schuldner sämtliche Vorkehrungen für die gültige Übertragung der Währungseinheiten getroffen hat und die massgebliche Transaktion mit sehr

---

127 Vgl. bitcoinwiki, Majority attack, <https://en.bitcoin.it/wiki/Majority_attack>. Das Risiko lässt sich mit dem Online-Tool <https://people.xiph.org/~greg/attack_success.html> anhand der Rechenleistung und der Anzahl Blöcke berechnen.

128 Vgl. PESCH, Cryptocoin-Schulden, S. 145 (unter Hinweis darauf, dass im März 2013 einige Miner eine unterschiedliche Version des Bitcoin-Protokolls ausführten, womit 32 Blöcke verwaist und die darauf gespeicherten Transaktionen ungültig wurden; im Juli 2015 akzeptierten Miner mit zusammen 50 % der Rechenleistung einen Block zu Unrecht als gültig und hängten an diesen eine Kette von sechs Blöcken an).

hoher Wahrscheinlichkeit im Netzwerk Bestand hat sowie gültig abgespeichert bleibt.[129]

Die technischen Anforderungen und die dafür erforderliche Zeitspanne variieren je nach der virtuellen Währung. Zu berücksichtigen sind insbesondere die gesamte im Netzwerk vorhandene Rechenleistung und deren Verteilung, die Art des Bestätigungsmechanismus der spezifischen Blockchain, der Schwierigkeitsgrad des zu lösenden kryptografischen «Puzzles»[130] und der Zeitbedarf bis zum Auffinden des nächsten Blocks.[131]

dd) Rechtsbehelfe bei gescheiterter Erfüllung

Lässt man für die Erfüllung einer Schuld und die Befreiung des Schuldners eine sehr hohe Wahrscheinlichkeit des Bestands der entsprechenden Transaktion im Netzwerk genügen, fragt sich, welche Rechtsbehelfe der Gläubigerin zustehen, wenn sie nach Abschluss der Erfüllung ihren Zugriff auf die übertragenen Werteinheiten infolge einer Veränderung der Blockchain-Datenbank verliert, insbesondere durch einen *Fork*. Weil das Schuldverhältnis mit der Erfüllung erlischt, kann die Gläubigerin nicht mehr die Erfüllung verlangen. Scheitert die Übertragung der virtuellen Währungseinheiten, ist anzunehmen, dass wieder der Schuldner oder ein Dritter in deren Besitz gelangt. Darin liegt eine *Bereicherung*. Diese dürfte ungerechtfertigt sein. Wenn die Transaktion zunächst in der Blockchain ihren Niederschlag gefunden hat, lässt sich die Auffassung vertreten, dass die Währungseinheiten vorübergehend der Gläubigerin zugestanden haben, weshalb diese durch die spätere Annullation entreichert worden ist. In der Regel liegt kein typischer Fall einer Leistungs- oder Eingriffskondiktion vor. In der Lehre werden ohne Rechtsgrund erfolgte Vermögensverschiebungen infolge des Verhaltens Dritter oder durch Zufall, das heisst durch ein äusseres Ereignis, häufig als

---

129 Vgl. PESCH, Cryptocoin-Schulden, S. 144 f., wonach entscheidend ist, «wann eine […] Transaktion objektiv hinreichend abgesichert ist» und «der massgebliche Verkehrskreis von einer ausreichenden Bestätigung ausgeht».

130 Bei einem *Proof-of-Work*-Konsensmechanismus darf derjenige Netzwerkteilnehmer einen neuen Block erstellen und darauf Transaktionen abspeichern, welcher als erster ein kryptografisches «Puzzle» löst. Das Bitcoin-System passt den Schwierigkeitsgrad des «Puzzles» automatisch so an, dass alle rund zehn Minuten ein neuer Block entsteht.

131 Vgl. PESCH, Cryptocoin-Schulden, S. 145 (je kleiner die Zeitspanne ist, desto leichter ist der Eintrag in der Blockchain kurzfristig korrumpierbar).

eigene Kategorie der ungerechtfertigten Bereicherung behandelt.[132] Der Erstattungsanspruch gemäss Art. 62 Abs. 1 OR geht grundsätzlich *in natura* auf erneute Übertragung der virtuellen Währungseinheiten, subsidiär auf Wertersatz in staatlicher Währung (vgl. zum Schadenersatz hinten, bei Fn. 170).

Demgegenüber geht eine deutsche Lehrmeinung mangels besonderer Vereinbarung der Parteien von einer vertraglichen Lücke aus. Diese ist nach dem hypothetischen Parteiwillen durch eine Vereinbarung zu füllen, wonach der *Erfüllungsanspruch* der Gläubigerin im Falle einer Verdrängung der Transaktion aus dem wesentlichen Strang der Blockchain wieder *aufleben* soll.[133] Befindet sich die Transaktion auf einem verwaisten Block, erlischt der Erfüllungsanspruch der Gläubigerin erst wieder durch das grundsätzlich automatisch erfolgende erneute Speichern und Validieren der Transaktion.[134] Eine Pflicht zu einem gezielten erneuten Auslösen der Transaktion durch den Schuldner, sofern beispielsweise der UTXO bereits für eine andere Transaktion genutzt worden ist, oder zu einem aktiven Monitoring der Transaktion lässt sich hingegen dem hypothetischen Parteiwillen ohne besondere Umstände nicht entnehmen.[135] Erst falls keine automatische erneute Transaktion erfolgt, verbleibt der Gläubigerin auch nach dieser Auffassung ein Anspruch aus ungerechtfertigter Bereicherung.

c) Ort der Erfüllung

Geldschulden sind gemäss Art. 74 Abs. 2 Ziff. 1 OR *Bringschulden*, das heisst am Ort zu zahlen, an welchem die Gläubigerin im Zeitpunkt der Erfüllung ihren Sitz oder Wohnsitz hat. Werden virtuelle Währungen als Zahlungsmittel eingesetzt, ist es vertretbar, die genannte Bestimmung analog anzuwenden und im Grundsatz ebenfalls eine Bringschuld anzunehmen. Bildet eine bestimmte Bitcoin-Münze den Gegenstand eines Vertrags, liegt der Erfüllungsort nach Art. 74 Abs. 2 Ziff. 2 OR am Lageort.

---

132 Vgl. BSK OR-SCHULIN, Art. 62 N 24 ff. m.w.H.

133 PESCH, Cryptocoin-Schulden, S. 147 f. m.w.H.

134 Vgl. PESCH, Cryptocoin-Schulden, S. 147 f. Eine Bitcoin-Transaktion auf einem verwaisten Block wird üblicherweise zurück in den «Mempool» (eine Art Transaktions-Warteraum) transferiert und auf einem neuen Block abgespeichert. Vor der Annahme eines erneuten Erfüllungsanspruchs ist nochmals eine gewisse Anzahl Blöcke abzuwarten, bis die Transaktion mit einer sehr hohen Wahrscheinlichkeit gültig gespeichert ist; insoweit offenbar a.M. PESCH, S. 148, wonach ein Erfüllungsanspruch gegebenenfalls nur für eine logische Sekunde auflebt und danach sofort wieder erlischt.

135 PESCH, Cryptocoin-Schulden, S. 148.

Bei einer Übertragung über das Blockchainsystem lässt sich indessen ein eigentlicher Erfüllungsort angesichts der dezentralen Struktur kaum bestimmen. Die Währungseinheiten sind in einer Datenbank gespeichert, verteilt auf ein Netzwerk bestehend aus einer Vielzahl an Computern. Entscheidend ist, dass der Schuldner der Gläubigerin die Verfügungsmacht über die Einheiten verschafft, so dass diese mittels ihres privaten Schlüssels darauf zugreifen kann. Die Frage des Erfüllungsorts ist dabei von geringer praktischer Relevanz. Bringschuld sollte immerhin bedeuten, dass grundsätzlich der Schuldner für die Registration der Transaktion im virtuellen Währungssystem verantwortlich ist und die Gläubigerin Verfügungsmacht über die transferierten Währungseinheiten erlangen kann, indem sie auf das System zugreift.

II. Verrechnung von virtuellen Währungen

1. Verrechnung gleichartiger virtueller Währungen

Schulden Parteien einander Geld oder sonstige gleichartige Leistungen, kann nach Art. 120 Abs. 1 OR jede Partei die erfüllbare eigene Schuld (Hauptforderung) mit ihrer fälligen Forderung (Verrechnungs- oder Gegenforderung) verrechnen. Handelt es sich bei den Leistungen um solche in derselben virtuellen Währung, ist die Verrechnung unabhängig davon möglich, ob die Schuld in virtueller Währung als «Geldsumme» qualifiziert wird. Denn es stehen sich «gleichartige» Leistungen gegenüber. Eine Umrechnung in eine staatliche Währung erübrigt sich.

2. Verrechnung unterschiedlicher Währungen

Weniger eindeutig ist die Rechtslage, wenn entweder zwei Forderungen in unterschiedlichen virtuellen Währungen oder eine Forderung in einer virtuellen Währung mit einer Forderung in einer staatlichen Währung verrechnet werden sollen. Nach der Praxis des Bundesgerichts zu Fremdwährungen ist die Verrechnung von Forderungen in unterschiedlichen Währungen zulässig, sofern nicht für eine Forderung eine Effektivleistung vereinbart ist.[136]

[136] BGE 130 III 312 E. 6.2 S. 318 m.w.H. In der Lehre ist die Verrechenbarkeit verschiedener Fremdwährungen strittig, vgl. die Hinweise bei BSK OR-PETER, Art. 120 N 11; ZK OR-SCHRANER, Art. 84 N 213. Die Vereinbarung einer Effektivklausel bewirkt nach der

Die Verrechnung setzt einen *Umrechnungskurs* zwischen den jeweiligen Währungen voraus. Dieser muss nach der Lehre bestimmbar[137] oder sogar allgemein anerkannt sein.[138] Massgeblich sein soll derjenige Kurs im Zeitpunkt des *Zugangs der Verrechnungserklärung*,[139] welchen der Verrechnungsgegner bei der Umwandlung in guten Treuen erzielt hätte.[140] Die Verrechnungsforderung ist umzurechnen nach dem Briefkurs der Hauptforderung.[141]

Ein offizieller oder allgemein anerkannter Umrechnungskurs existiert bei virtuellen Währungen nicht. Der Kurs der betroffenen virtuellen Währung ergibt sich bei den gängigen Handelsplattformen grundsätzlich aus Angebot und Nachfrage. Da das Zusammenspiel von Angebot und Nachfrage je nach Handelsplattform und Zeitpunkt variiert, sind die Umrechnungskurse uneinheitlich. Auch wenn die Differenzen bei häufig gehandelten virtuellen Währungen abgenommen haben und teilweise durch Arbitrage-Geschäfte ausgeglichen werden, können sie ins Gewicht fallen. Bei Bitcoin, der virtuellen Währung mit der höchsten Marktkapitalisierung, hat der Unterschied zwischen den beiden Plattformen mit dem grössten Handelsvolumen bei einer von zwei Stichproben über 1 % betragen.[142] Bei seltener gehandelten virtuellen Währungen sind die Differenzen teilweise deutlich grösser. Der Handel ist oft fragmentierter als bei staatlichen Währungen. Gewisse Platt-

---

Lehre ein Verrechnungsverbot gemäss Art. 126 OR, indem die geschuldeten Leistungen nicht gleichartig sind.

137 BK OR-ZELLWEGER-GUTKNECHT, Art. 120 N 216 (dass ein Kurs bestritten ist, schadet nicht).

138 ZK OR-SCHRANER, Art. 84 N 213 f.

139 BK OR-WEBER, Art. 84 N 343; nach abweichender Auffassung wird auf den Moment abgestellt, ab welchem sich die Forderungen verrechenbar gegenübergestanden sind, BK OR-ZELLWEGER-GUTKNECHT, Art. 120 N 218 m.w.H.

140 ZK OR-SCHRANER, Art. 84 N 215 m.w.H.

141 BK OR-ZELLWEGER-GUTKNECHT, Art. 120 N 217 (der Verrechnungsgegner muss gewissermassen die Verrechnungsforderung verkaufen und behält Währung der Verrechnungsforderung; er könnte sich damit die entgangene Währung der Hauptforderung zum Verkaufspreis der Banken beschaffen; zur Terminologie BK OR-ZELLWEGER-GUTKNECHT, Vorbem. Art. 120–126 N 23 f.).

142 Kurs vom 30. Januar 2018 um 09.26 Uhr (Differenz 1,23 %): Bitfinex USD 11'129.00, GDAX USD 10'993.00; Kurs vom 17. April 2018 um 22.11 Uhr (Differenz 0,05 %): Bitfinex USD 7'882.10, GDAX USD 7'878.00. Quelle: CryptoCompare, Bitcoin USD Live Exchange Prices and Volumes, <www.cryptocompare.com/coins/btc/markets/USD>.

formen sind spezifisch geografisch, etwa auf den asiatischen[143] oder indischen[144] Markt, ausgerichtet. Auf diese Weise können sich regionale Einflüsse, darunter regulatorische Massnahmen, in konzentrierter Form bemerkbar machen. Plattformspezifische Nachfrage- und Angebotsüberhänge bewirken dabei eine Abweichung von den Kursen anderer Handelsplattformen.

Für *Steuerzwecke* errechnete die Eidgenössische Steuerverwaltung (ESTV) beim Steuerjahr 2016 einen Durchschnittskurs von CHF 977.53 pro Bitcoin anhand der Daten von fünf Websites,[145] darunter Finanzportale[146] und Nachrichtenanbieter mit Fokus auf Blockchaintechnologie.[147] Die Auswahl der Datenanbieter erscheint eher zufällig.[148] Anstatt sich auf private Dienstleister, deren Kursbewertungsmodelle nicht immer transparent sind, abzustützen, ist es bei verbreiteten und häufig gehandelten virtuellen Währungen[149] zweckmässiger, direkt die Durchschnittskurse einer gewissen Anzahl Plattformen mit den grössten Handelsvolumen heranzuziehen.[150] Dies wurde für das Steuerjahr 2017 zumindest teilweise gemacht.[151] Zustimmung verdient, jeweils den höchsten und den niedrigsten Kurs für die Berechnung auszuklammern. Wegen der hohen (Tages-)Volatilität sollte – zumindest *de lege ferenda* – nicht bloss auf einen einzigen Zeitpunkt abgestellt werden, etwa den 31. Dezember um 24.00 Uhr Schweizer Zeit.[152] Es sei an die frühere Praxis erinnert, wonach die Kurse von Wertschriften nach

143 Zum Beispiel Huobi.pro mit Hauptsitz in Singapur, <www.huobi.pro/zh-cn>.

144 Etwa Koinex in Mumbai, <https://koinex.in>.

145 NATALIE GRATWOHL, Wie Bitcoins besteuert werden, NZZ 28. Dezember 2016; PILLER, AJP 2017, S. 1432 mit Fn. 75.

146 <Oanda.com>, <ariva.de> und <investing.com>.

147 <Coindesk.com> und <bitcoin.de>.

148 TOBIAS F. ROHNER/CHRISTIAN JAAG, Wie Kryptowährungen zu besteuern sind, NZZ 4. Januar 2017.

149 Dazu gezählt werden können derzeit etwa Bitcoin, Ether, Ripple, Bitcoin Cash, Litecoin oder Ether Classic.

150 LINDER/MEYER, Zürcher Steuerpraxis 2017, S. 202.

151 Die nicht veröffentlichte Kursliste der ESTV zur Empfehlung an die kantonalen Steuerbehörden bestimmt die Umrechnungskurse per Ende 2017 je nach virtueller Währung anhand von drei (für IOTA) bis 13 (für Bitcoin) Quellen, wobei auch Handelsplattformen einbezogen werden.

152 Der Unterschied zwischen Tagestief und -hoch schwankte bei Bitcoin im Januar 2018 zwischen rund 4,7 % und 26,4 %; der Durchschnitt lag bei 9,7 % (berechnet anhand der Angaben von CoinMarketCap, Historical data for Bitcoin, <https://coinmarketcap.com/currencies/bitcoin/historical-data>).

dem Durchschnitt des gesamten Monats Dezember bestimmt worden sind.[153] Falls ein Investor virtuelle Währungen erst im Verlaufe des Monats erworben hat, ist allerdings nur die tatsächliche Haltedauer zu berücksichtigen.

Auch für die Zwecke einer Verrechnung erschweren die erheblichen Kursschwankungen und die Unterschiede zwischen einzelnen Handelsplattformen die Festlegung des Umrechnungskurses. Von Bedeutung ist in diesem Zusammenhang der massgebliche Zeitpunkt. Wird auf den Zugang der Verrechnungserklärung abgestellt (vorne, bei Fn. 139), fragt sich, ob sich so eine exakte Uhrzeit bestimmen lässt.[154] Steht lediglich der Kalendertag fest, kann auf den *Tagesmittelkurs* abgestellt werden. Der Tagesmittelkurs lässt sich beispielsweise anhand von Stundenintervallen bilden. Dies bedeutet, dass der Kurs erst am Ende des Tages – *nach* der Übermittlung der Verrechnungserklärung – berechnet werden kann. Der Vorteil eines derartigen Tagesmittelkurses gegenüber dem Endkurs um Mitternacht gemäss der Lokalzeit der entsprechenden Plattformen liegt darin, dass zufällige Intraday-Schwankungen geglättet werden und überdies vermieden wird, dass der Endkurs in Asien und den USA, wo sich die grössten Handelsplattformen für virtuelle Währungen befinden, wegen der Zeitverschiebung unterschiedliche Zeiten abbildet. Es empfiehlt sich, mindestens drei gängige Plattformen heranzuziehen. Eine lokale Ausrichtung nach dem Sitz oder Wohnsitz des Verrechnungsgegners erscheint für die Auswahl der Plattformen nicht geboten.

Die Schwierigkeiten bei der Kursbestimmung und der zeitlichen Festsetzung der Umrechnung zeigen, dass die Möglichkeit der Verrechnung virtueller Währungen nicht unproblematisch ist. Als einseitiges Rechtsgeschäft

---

153 Vgl. Art. 15 Abs. 4 Satz 2 der bis Ende 2013 geltenden Fassung des Bundesgesetzes über die Harmonisierung der direkten Steuern der Kantone und Gemeinden (StHG) vom 14. Dezember 1990 (SR 642.14), wonach in der Schweiz gehandelte Wertpapiere mit Kurswert nach dem Durchschnitt der Kurse im letzten, dem Beginn der Steuerperiode oder der Steuerpflicht vorangehenden Monat bemessen worden sind.

154 Gemäss der absoluten oder uneingeschränkten Empfangstheorie wird bei mittelbaren Erklärungen, welche vor dem Empfang übermittelt werden, für den Zugang im Allgemeinen auf den Zeitpunkt abgestellt, in welchem die Erklärung in den Machtbereich des Empfängers oder seines Vertreters gelangt, sodass der Empfänger bei normaler Organisation seiner Verhältnisse in der Lage ist, von der Erklärung Kenntnis zu nehmen, vgl. zur Fristberechnung im Mietrecht BGE 140 III 244 E. 5.1 S. 247. Für die Berechnung von Fristen genügt grundsätzlich die Bestimmung des Tages.

sollte die Verrechnung den Verrechnungsgegner als Schuldner der Verrechnungsforderung und Gläubiger der Hauptforderung nicht benachteiligen. Indem die verrechnende Partei über die Verrechnung bestimmt und den Zeitpunkt der Umrechnung der Verrechnungsforderung steuern kann, lässt sich das Risiko einer Benachteiligung nicht ausschliessen. Im Einklang mit der Beurteilung unter Art. 84 Abs. 2 OR ist bei der Verwendung virtueller Währungen mangels gegenteiliger Abrede die Vereinbarung der *effektiven Leistung* zu vermuten (vorne, bei Fn. 113).[155] Insoweit entfällt die Möglichkeit der Verrechnung (vorne, bei Fn. 136). Von vornherein verfehlt wäre eine Verrechnung, wenn die virtuelle Währung nicht als Zahlungsmittel verwendet und die Übertragung nicht einem Entgelt dient, sondern etwa zu Investitionszwecken, sodass die Gläubigerin die Leistung der virtuellen Währung «effektiv» erwartet. Zu bejahen ist die Verrechnungsmöglichkeit demgegenüber bei *stable coins*, deren Wert an eine staatliche Währung gebunden ist, sofern die Parteien nicht die effektive Leistung vereinbart haben (vgl. vorne, bei Fn. 114).

III. Leistungsstörungen bei virtuellen Währungen

Bilden virtuelle Währungen den Gegenstand von Verträgen, ist auch die Rechtslage bei Leistungsstörungen zu erörtern. Im Grundsatz finden die allgemeinen Bestimmungen Anwendung, doch ergeben sich einige Besonderheiten. Nachfolgend wird untersucht, ob die Gläubigerin bei Leistungsverzögerungen Verzugszinsen oder die Erfüllung in staatlicher Währung verlangen kann (III.1), inwieweit eine Unmöglichkeit denkbar ist beziehungsweise welche Rechtsfolgen eintreten (III.2) und wie Schadenersatzansprüche zu handhaben sind (III.3).

[155] Für Zulässigkeit der Verrechnung einer Forderung in Bitcoin, sofern eine sachgerechte Umrechnungsmethode angewandt wird, PILLER, AJP 2017, S. 1432.

1. Verzug

a) Verzugszinsen

Gerät der Schuldner einer Leistung in virtueller Währung in Verzug, stellt sich die Frage, ob es sich um die «Zahlung einer Geldschuld» gemäss der dispositiven Regelung von Art. 104 Abs. 1 OR handelt, sodass nach der Inverzugsetzung ein Verzugszins in der Höhe von 5 % geschuldet ist. Eine Auslegung nach dem Wortlaut führt nicht zu einem schlüssigen Resultat. Bezieht sich der Leistungsgegenstand auf bestimmte Banknoten oder Münzen in Franken (Stückschuld), wird die Anwendung von Art. 104 Abs. 1 OR verneint,[156] obwohl es sich um Geld im Sinne der gesetzlichen Zahlungsmittel handelt. Forderungen in Fremdwährungen unterstehen Art. 104 OR.[157] Vorauszusetzen ist die Anwendbarkeit des schweizerischen Rechts.[158] Demgegenüber wird ein Verzugszins bei WIR abgelehnt, solange die Schuld nicht im Rahmen der Vollstreckung in Franken umgerechnet worden ist.[159] Zentral erscheinen teleologische Aspekte: Es geht beim Verzugszins um eine Entschädigung der Gläubigerin für die vorenthaltene Geldleistung und um die Erstattung eines etwaigen vom Schuldner bezogenen Nutzens.[160] Die zugrunde liegende Erwartung ist somit, dass die Gläubigerin die Geldsumme während des Verzugs hätte zinsbringend anlegen können und umgekehrt der Schuldner noch Zinsen dafür in Empfang nehmen konnte, welche eigentlich der Gläubigerin zustehen würden. Nicht bezweckt wird der Ersatz eines von der Gläubigerin nachweislich erlittenen Vermögensverlusts. Übersteigt der Schaden die Verzugszinsen, kann die Gläubigerin diesen gestützt auf Art. 106 Abs. 1 OR zusätzlich geltend machen, sofern dem Schuldner nicht der Exkulpationsbeweis gelingt.

---

156 BK OR-WEBER, Art. 104 N 53 (Anwendung beschränkt auf Geldsummenschuld).

157 BK OR-WEBER, Art. 104 N 54.

158 Kollisionsrechtlich ist bei der Verzinsung umstritten, ob für diese das Schuld- oder das Währungsstatut massgeblich ist, vgl. BSK IPRG-DASSER, Art. 147 N 8b m.w.H. Obwohl sich die Höhe einer Schuld gemäss Art. 147 Abs. 2 IPRG grundsätzlich nach dem auf die Schuld anwendbaren Recht bestimmt, ist zu bedenken, dass die Verzinsung wirtschaftlich von der Währung abhängt. So kann sich eine Abweichung vom Schuldstatut aufdrängen und die Anwendung des Währungsstatuts empfehlen, falls ein solches existiert.

159 BK OR-WEBER, Art. 104 N 55.

160 BK OR-WEBER, Art. 104 N 7 m.w.H.

Derzeit ist eine zinstragende Verwahrung von virtuellen Währungen nicht üblich. Die Möglichkeit des Zinsdifferenz- beziehungsweise Fristentransformationsgeschäfts analog zur Banktätigkeit entfällt, solange virtuelle Währungen nicht Dritten als Kredit zur Verfügung gestellt werden. Unter Umständen hätte die Verzinsung regulatorische Implikationen.[161] Ohnehin widerspricht der Einbezug von Banken oder anderen Intermediären, obgleich verschiedentlich anzutreffen, der dezentralen Struktur eines Blockchainsystems. Insgesamt muten Zinsen im Bereich der virtuellen Währungen aus heutiger Sicht «systemwidrig» an. Es ist anzunehmen, dass die Gläubigerin wegen der verzögerten Leistung keiner Zinsen verlustig geht und dem Schuldner für die vorenthaltene virtuelle Währung während des Verzugs keine Zinsen zukommen. Ein zeitlicher Aufschub lässt wegen der unsicheren Wertentwicklung auch nicht *per se* erwarten, dass der Schuldner die virtuelle Währung günstiger beschaffen kann. Dass die Gläubigerin die virtuellen Währungseinheiten im Falle einer früheren Erfüllung der Schuld in staatliche Währung hätte umwechseln und zinstragend anlegen können, spielt keine Rolle und könnte auch bei Stückschulden geltend gemacht werden. Verzugszinsen gemäss Art. 104 Abs. 1 OR sind bei einer Schuld in virtueller Währung grundsätzlich *abzulehnen.*[162] Es fehlt an einer «Geldschuld» im hier verstandenen Sinne beziehungsweise es ist ein stillschweigender Ausschluss der Verzugszinsen anzunehmen. Diese Auffassung bedeutet, dass im Einzelfall genau zu prüfen ist, ob eine primäre oder alternative Schuld in staatlicher Währung besteht, für welche Verzugszinsen geschuldet sind. Vorbehalten bleiben Schadenersatzansprüche gestützt auf Art. 103 Abs. 1 OR, sofern der Schuldner den Verzugseintritt verschuldet hat (hinten, III.3.b).

Wiederum ist die Situation bei *stable coins* (vorne, I.2.e.ee), deren Wert an eine staatliche Währung gebunden ist, abweichend zu beurteilen. Hier stellt die virtuelle Währung eine Art Surrogat für die entsprechende Fremdwährung dar. Erfolgt die Ausgabe gegen Hinterlegung staatlicher Währung,

---

161 Vgl. für Abwicklungskonti Art. 5 Abs. 3 lit. c und für die Entgegennahme von Publikumseinlagen von höchstens CHF 1 Mio. Art. 6 Abs. 2 lit. b Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV) vom 30. April 2014 (SR 952.02).

162 Gl.M. GOBAT, AJP 2016, S. 1100 (zu Bitcoin; Verzugszinsen jedoch nach Wechsel der Forderung in Franken im Zuge einer Betreibung); MIGNON, Jusletter 4. Mai 2015, Rz. 147 (Verzugszinsen aufgrund einer vertraglichen Vereinbarung möglich); a.M. PILLER, AJP 2017, S. 1431 (zu Bitcoin; höhere Zirkulationsfähigkeit beziehungsweise Liquidität im Vergleich zu WIR).

kann der Schuldner zwar kaum Zinsen empfangen, falls er den geschuldeten Betrag bereits in der virtuellen Währung hält. Doch kämen der Gläubigerin bei der Rücknahme der «Stammwährung» – beispielsweise US-Dollar – unter Umständen Zinsen zu. Die Umwechslung liegt bei *stable coins* mit Anbindung an die betreffende staatliche Währung näher als bei den übrigen virtuellen Währungen. Die analoge Anwendung von Art. 104 OR erscheint gerechtfertigt.

b) Geltendmachung der Forderung in staatlicher Währung?

Bei einem Kaufpreis, welcher in Franken festgesetzt ist, aber vollständig in WIR bezahlt werden soll, darf die Gläubigerin gemäss Bundesgericht wie erwähnt (vorne, bei Fn. 102) die Zahlung in Franken verlangen, falls die vertraglich zugelassene Leistung in WIR nicht zur Tilgung der Schuld führt. Dies gilt auch für den Fall, dass der Schuldner seine Schuld nicht rechtzeitig erfüllt. Die WIR Bank Genossenschaft sieht in ihren Geschäfts- beziehungsweise Teilnahmebedingungen, deren Anwendung in dem vom Bundesgericht beurteilten Fall umstritten gewesen ist, nach erfolgloser Mahnung ausdrücklich eine «Umrechnung» der WIR-Schuld in Franken im Verhältnis 1:1 vor.[163] Folgt man der bundesgerichtlichen Auffassung, wird die Schuld nicht umgewandelt, sondern lautet die ursprünglich geschuldete Leistung auf Franken. Der Verzug beendet die Stundung, sodass die Gläubigerin die Erfüllung in Franken verlangen darf.

Wie die Rechtslage bei WIR zeigt, sind die getroffenen Vereinbarungen entscheidend. Wer virtuelle Währungen über eine Plattform erwirbt, möchte nicht, dass die Forderung in staatlicher Währung erfüllt wird. Der Schuldner ist nicht berechtigt, seine Schuld in Franken zu erfüllen. Geschuldet bleibt

[163] Ziff. C.8 lit. b AGB WIR (Fn. 32): «Wird eine fällige WIR-Zahlung nicht fristgemäss beglichen, so hat der rechnungsstellende WIR-Teilnehmer seinen Vertragspartner mittels Mahnung in Verzug zu setzen. Wird die Forderung in WIR nicht innert einer Frist von 7 Tagen seit Zugang der Mahnung beglichen, ist der WIR-Betrag vollumfänglich in CHF (umgerechnet in einem 1:1-Verhältnis von CHW zu CHF) geschuldet. Die Bank empfiehlt, die Mahnung schriftlich mit Zustellnachweis zu versenden und den Betrag frühestens 5 Tage, nachdem die Frist von 7 Tagen seit Zugang der Mahnung abgelaufen ist, allenfalls in Betreibung zu setzen.»; ebenso Ziff. 8 lit. b Teilnahmebedingungen WIR (Fn. 32). Eine analoge Regelung gilt gemäss Ziff. C.2 Abs. 2 AGB WIR (Ziff. 2 Abs. 2 Teilnahmebedingungen WIR) gegenüber der WIR Bank für den Fall von Kontoüberzügen in WIR: Der WIR-Teilnehmer schuldet der Bank den Saldo nach Ablauf der angesetzten Frist in Schweizer Franken.

auch im Verzugsfall die Leistung in virtueller Währung, es liegt kein Erfüllungssurrogat vor.

Anders ist die Situation in der Regel, falls virtuelle Währungen als Zahlungsmittel eingesetzt werden. Legen die Parteien ein Entgelt in Franken oder in einer anderen staatlichen Währung fest und gibt die Gläubigerin ausdrücklich oder konkludent zu verstehen, «auch» eine Zahlung in bestimmten virtuellen Währungen zu akzeptieren, besteht eine Verwandtschaft mit der erwähnten Zahlungsmöglichkeit in WIR. Bei einer etablierten virtuellen Währung ist es kaum denkbar, dass der Zahlungsvorgang an äusseren Umständen scheitert. Doch ist im Verzugsfall auch ohne ausdrückliche Vereinbarung davon auszugehen, dass die Gläubigerin die Leistung des Entgelts in der vereinbarten staatlichen Währung verlangen darf. So betrachtet fallen auch Verzugszinsen an.

Umgekehrt ist denkbar, dass der Preis für Waren oder Dienstleistungen einzig in einer virtuellen Währung festgesetzt wird und keine ursprüngliche Schuld in staatlicher Währung besteht. Fehlt es an besonderen Vereinbarungen für den Verzugsfall, kommt eine Umwandlung der virtuellen Währung in eine staatliche Währung kaum in Frage. Es fehlt hierfür an einer Rechtsgrundlage, sofern auch keine stillschweigende Parteivereinbarung angenommen werden kann. Daraus folgt, dass im Interesse der Gläubigerin der Preis stets in staatlicher Währung festgesetzt werden sollte. Dies empfiehlt sich auch mit Blick auf die Wertschwankungen virtueller Währungen. Ohne gegenteilige Abrede liegt eine Leistung erfüllungshalber vor, doch kann die Leistung in virtueller Währung auch an Zahlungs statt (vgl. vorne, Fn. 101) vorgesehen werden.

2. Unmöglichkeit der Erfüllung

Zeigt sich, dass die Erfüllung einer Schuld in virtueller Währung bereits im Zeitpunkt der Begründung der Schuld *objektiv* nicht möglich ist, liegt Nichtigkeit gemäss Art. 20 OR vor. Davon zu unterscheiden ist die nachträgliche objektive Unmöglichkeit im Sinne von Art. 119 Abs. 1 OR. Von einer solchen ist auszugehen, wenn die Übertragung von Werteinheiten der vereinbarten virtuellen Währung *generell* unmöglich geworden ist.[164] Dies wäre denkbar, wenn aufgrund eines technischen Fehlers im Protokoll einer Blockchain oder in der darauf aufbauenden Applikation keine Einheiten der virtuellen Wäh-

[164] Näher zur Unmöglichkeit bei Gattungsschulden BSK OR-WIEGAND, Art. 97 N 20.

rung mehr übertragen werden könnten oder wenn kein Netzwerkknoten die zugrunde liegende Blockchain noch unterhielte.[165] Hat der Schuldner die Unmöglichkeit nicht zu verantworten, erlischt die Forderung auf Leistung der virtuellen Währung. Der Schuldner wird befreit und hat bei zweiseitigen Verträgen gemäss Art. 119 Abs. 2 OR bereits erhaltene Gegenleistungen zurückzuerstatten.

Aufgrund des Charakters als Gattungsschuld führt eine *subjektive* Unmöglichkeit der Erfüllung einer auf virtuelle Währung lautenden Schuld, beispielsweise aufgrund der Mittellosigkeit des Schuldners, nicht zum Erlöschen der Forderung. Die Gläubigerin kann an der nachträglichen Erfüllung der Forderung festhalten. Der Schuldner haftet gestützt auf Art. 97 OR beziehungsweise Art. 103 Abs. 1 und Art. 107 Abs. 2 OR.[166] Ausnahmen von der Qualifikation als Gattungsschuld sind denkbar, wenn die Lieferung spezifischer Werteinheiten einer virtuellen Währung vereinbart worden ist.

Ein starker Anstieg des Kurses einer virtuellen Währung führt nicht zu einer objektiven Unmöglichkeit der Leistung. Stehen die für die Erfüllung erforderlichen Aufwendungen in keinem vernünftigen Verhältnis zum Wert der Leistung, kann die derartige Unerschwinglichkeit unter Umständen wie eine subjektive Unmöglichkeit behandelt werden. Überdies könnte ein Gericht in Anwendung der *clausula rebus sic stantibus* eine Vertragsanpassung vornehmen (vorne, bei Fn. 22). Allerdings sind starke Kursschwankungen bei den meisten virtuellen Währungen allgemein bekannt sowie voraussehbar (vorne, bei Fn. 50).

3. Schadenersatzanspruch

a) Massgebliche Währung

Die vertragliche Haftung richtet sich grundsätzlich nach Art. 97 ff. OR. Gemäss Art. 99 Abs. 3 i.V.m. Art. 43 Abs. 1 OR bestimmt das Gericht die Art und den Umfang des Schadenersatzes. Dem Gericht kommt dabei Ermessen zu. Massgeblich sind die Umstände des Einzelfalls. Fraglich ist vorliegend, ob beziehungsweise wann der Schadenersatz in virtueller Währung zu leisten ist.

---

165 Vgl. zur Unmöglichkeit unter deutschem Recht PESCH, Cryptocoin-Schulden, S. 160 f. m.w.H.

166 BSK OR-WIEGAND, Art. 97 N 11 und 13 m.w.H.

Das Bundesgericht hält bei vertraglichen Schadenersatzansprüchen unter Berufung auf die Lehre grundsätzlich die Währung des Staates für massgeblich, in welchem der Vermögensschaden eingetreten ist, unter Umständen aber auch die vertraglich vereinbarte Währung *(«monnaie du contrat»)*, insbesondere wenn der Anspruch auf Schadenersatz an die Stelle einer vertraglichen Zahlungspflicht tritt, beispielsweise eines Lohns oder einer Vergütung.[167] So lautet der Schadenersatz aus dem versäumten Verkauf von Optionen in US-Dollar seinerseits auf US-Dollar.[168] Das Schadenersatzbegehren muss die entsprechende Währung nennen und darf bei einer Fremdwährung nicht bloss den umgerechneten Betrag in Franken anführen. Die strikte Haltung der Gerichte, welche sich an die Parteianträge gebunden fühlen, ist in der Lehre auf Kritik gestossen.[169] Oft wäre für die geschädigte Partei mit Sitz oder Wohnsitz in der Schweiz die Zusprechung von Schadenersatz in Franken gerechtfertigt, auch wenn ursprünglich eine Fremdwährungsschuld vereinbart wurde beziehungsweise den Vertragsgegenstand bildete.

Bei virtuellen Währungen ist eine örtliche Anknüpfung an den Schadensort ausgeschlossen, zumindest solange nicht ein Staat eine virtuelle Währung mit territorial begrenztem Anwendungsgebiet ausgegeben beziehungsweise eine virtuelle Währung für sein Land als gesetzliches Zahlungsmittel anerkannt hat. Ausserdem erscheint ein starres Abstellen auf die vereinbarte virtuelle Währung nicht als sachgerecht, selbst wenn diese als ausschliessliches Entgelt dienen soll. Auch mit Blick auf die Vollstreckung eines Urteils und die Problematik der Kursschwankungen sollte es dem Geschädigten offenstehen, Schadenersatz in staatlicher Währung zu verlangen.[170] Dass Schadenersatz aber auch in Form einer virtuellen Währung zugesprochen werden kann, ergibt sich bereits aus der Möglichkeit der

---

167 BGer Urteile 4A_341/2016 und 4A_343/2016 vom 10. Februar 2017 E. 2.2; BGE 137 III 158 E. 3.2.2 S. 161 *(«appare sensato provvedervi mediante la valuta nella quale la diminuzione del patrimonio si è realizzata»);* vgl. auch BSK OR-KESSLER, Art. 43 N 2 (Geldersatz ist in jener Währung geschuldet, in der die Vermögensmasse geführt wird, in welcher der Schaden eingetreten ist).

168 BGer Urteil 4C.191/2004 vom 7. September 2004 E. 6, mit Verweis auf ZK OR-SCHRANER, Art. 84 N 181 (in der Regel Währung des Staates, in dessen Gebiet der Vermögensschaden eingetreten ist, unter Umständen Schuldwährung).

169 KOLLER, Anwaltsrevue 2017, S. 266.

170 Vgl. PILLER, AJP 2017, S. 1431 (Schadenersatz in Bitcoin oder Franken).

Naturalrestitution unter Art. 43 OR.[171] Somit besteht kein Bedarf, Schulden in virtuellen Währungen für den Zweck von Schadenersatzansprüchen wie Schulden in Fremdwährungen zu behandeln.

b) Ersatz von Kursverlusten

Die Zufallshaftung gemäss Art. 103 Abs. 1 OR mit der Möglichkeit des Exkulpationsbeweises erfasst grundsätzlich auch Kursverluste, welche bei der geschuldeten virtuellen Währung eintreten. Die Gläubigerin soll in denjenigen Vermögensstand gesetzt werden, welcher bestünde, falls die Schuld rechtzeitig erfüllt worden wäre. Der Schadensnachweis obliegt der Gläubigerin. Behauptet die Gläubigerin, durch die verspätete Leistung des Schuldners Währungsverluste erlitten zu haben, muss sie den Beweis erbringen, dass sie den Betrag bei rechtzeitiger Erfüllung umgehend in eine andere Währung umgewandelt hätte.[172] Die Rechtsprechung zu Kursverlusten bei Fremdwährungen geht gestützt auf die allgemeine Lebenserfahrung und den gewöhnlichen Lauf der Dinge von der Vermutung aus, dass die Gläubigerin das Geld bei Fälligkeit in die gesetzliche Währung ihres Wohn- oder Geschäftssitzes konvertiert hätte.[173] Diese natürliche Vermutung erleichtert den Schadensnachweis, kommt gemäss Bundesgericht aber weder einer Umkehr der Beweislast noch einer abstrakten Schadensberechnung gleich.[174] Macht die Gläubigerin eine Differenz zu einer anderen als ihrer Landeswährung geltend, obliegt ihr der Nachweis, dass sie den geschuldeten Betrag in jene Währung gewechselt hätte.

Virtuelle Währungen unterscheiden sich stärker als Fremdwährungen von der staatlichen Währung am Sitz der Gläubigerin. Eine generelle Vermutung, dass die Gläubigerin die virtuellen Währungseinheiten in die staatliche Währung umwandelt, erscheint nicht gerechtfertigt, zumal virtuelle

---

171 Dazu etwa BK OR-BREHM, Art. 43 N 19 ff.

172 BGE 123 III 241 E. 3a S. 243.

173 So bereits BGE 109 II 436 E. 2 S. 440 ff.; eingehend zur Rechtslage bei Währungs- und Kursverlusten und zu den der Gläubigerin gewährten Beweiserleichterungen BK OR-WEBER, Art. 106 N 25 ff. m.w.H.

174 In ähnlicher Weise lässt sich gestützt auf die allgemeine Lebenserfahrung vermuten, dass ein Finanzinstitut einen bei ihr eingehenden Geldbetrag, welcher nicht für den laufenden Geschäftsbetrieb erforderlich ist, zinstragend angelegt hätte, vgl. BGE 123 III 241 E. 3b S. 244 m.w.H. Der Schuldner kann den Gegenbeweis antreten und darlegen, dass der Erfahrungsschluss aufgrund untypischer Umstände nicht berechtigt sei.

Währungen üblicherweise global verwendet werden können. Überdies ist die Umrechnung in die staatliche Währung mit Schwierigkeiten verbunden. Deshalb ist grundsätzlich von der Gläubigerin zu beweisen, inwieweit sie den Betrag in die staatliche oder eine andere Währung gewechselt hätte. Problemlos wird ein derartiger Nachweis einem Anbieter von Waren oder Dienstleistungen gelingen, welcher lediglich zur Steigerung seiner Attraktivität auch gewisse virtuelle Währungen als Zahlungsmittel akzeptiert (vgl. vorne, bei Fn. 117) und diese stets umgehend in die staatliche Währung seines Geschäftssitzes umwandelt. Ebenso liegt bei einem Nutzer von *stable coins* (vorne, I.2.e.ee), deren Wert an eine staatliche Währung gebunden ist, die Annahme nahe, dass er die erhaltenen virtuellen Währungseinheiten in die entsprechende staatliche Währung zurückwechselt.

IV. Zwangsvollstreckung bei virtuellen Währungen

1. Schuldbetreibung

a) Historischer Hintergrund des Betreibungsverfahrens

Bereits lange vor dem Inkrafttreten des Bundesgesetzes über Schuldbetreibung und Konkurs im Jahr 1892 existierten Gantverfahren zur Vollstreckung einzelner Vermögensstücke eines Schuldners. Dem mittellosen Schuldner drohten Schuldhaft sowie Landesverweisung.[175] In der Stadt Zürich war eine Geldschuld gestützt auf den Richtebrief (Stadtrecht) aus der zweiten Hälfte des 14. Jahrhunderts beim Gericht des Schultheissen oder Vogtes einzuklagen, während die Vollstreckung des Urteils – im Gegensatz zu anderen Städten – nicht diesem Gericht, sondern dem Rat oblag.[176] Der Rat verfügte über mehr Macht, und ihm oblag auch die Strafgerichtsbarkeit. Der Rat forderte den Schuldner nochmals auf, dem Urteil Folge zu leisten und innerhalb eines Monats zu zahlen. Auf Ersuchen des Klägers wurde der Schuldner anschliessend zu einer Busse zwischen einem Pfund und fünf Schilling verurteilt, abhängig von der Grösse der Schuld. Nach zwei weiteren Fristen

[175] Botschaft SchKG, S. 42. Das Konkursverfahren entwickelte sich in den kantonalen Rechtsordnungen erst später, und zwar ursprünglich für besitzlose und flüchtige Schuldner, bei denen die Durchführung der Pfändung nicht möglich war oder ohne Erfolg blieb.

[176] VON WYSS, ZSR 1858, S. 9 f.

von je vierzehn Tagen durfte der Kläger beim Rat die Pfändung verlangen.[177] Konnten beim Schuldner nicht genügend Vermögenswerte vorgefunden werden, wurde dieser aus der Stadt verwiesen.[178]

Das Betreibungsverfahren war auch im 19. Jahrhundert auf Geldforderungen ausgerichtet und wurde von der sonstigen Vollstreckung getrennt.[179] Immerhin war es in einigen Kantonen möglich, eine Forderung auf eine sonstige Leistung in Geld zu schätzen und den Schuldner alternativ auf die ursprüngliche Verpflichtung oder auf Zahlung der Schätzungssumme zu betreiben.[180] Im Kanton Bern hingegen musste bei der Betreibung von ursprünglich nicht auf Geld gerichteten Forderungen wegen des Problems der einseitigen Schätzung der Forderungshöhe das Gericht den Geldbetrag festsetzen.[181] Obwohl der Schuldner eine gerichtliche Beurteilung bewirken kann, indem er die Forderung bestreitet, ist die aussergerichtliche Zwangsexekution von Geldforderungen anfänglich nicht unumstritten gewesen.[182] Aufgrund ihrer Einfachheit und des prozessökonomischen Nutzens hat sie jedoch bis heute überdauert.

Auch nach heutigem Recht unterliegt abgesehen von Sicherheitsleistungen lediglich die Zwangsvollstreckung von Geldforderungen der Schuldbetreibung (vgl. Art. 38 Abs. 1 SchKG). Der bewusst enge Anwendungsbereich des Schuldbetreibungsrechts gemäss SchKG bewahrte die Kompetenz der Kantone für die Realexekution, denn Letztere wurde bis zum Inkrafttreten

---

177 VON WYSS, ZSR 1858, S. 10. In der Folgezeit trat an die Stelle der dreimaligen Zahlungsaufforderung eine einzige.

178 Dadurch verlor der Schuldner den Schutz der Stadt. Er durfte vom Gläubiger zur Befriedigung der Schuld aufgegriffen werden.

179 Die Vollstreckung anderer Ansprüche hing von der Art des Begehrens ab. In Frage kam die direkte Vollziehung, andernfalls die Verhängung einer Strafe als indirektes Zwangsmittel, VON WYSS, ZSR 1858, S. 84.

180 Diese Möglichkeit sahen die Gesetze der Kantone Zürich, Schaffhausen, Solothurn und Thurgau vor, VON WYSS, ZSR 1858, S. 84.

181 VON WYSS, ZSR 1858, S. 85.

182 Dass darin aus rechtswissenschaftlicher Sicht eine *«singuläre Barbarei»* gesehen werden könnte, betont der Rechtshistoriker FRIEDRICH VON WYSS im Jahr 1858, VON WYSS, ZSR 1858, S. 3.

der Schweizerischen Zivilprozessordnung (ZPO)[183] in den kantonalen Zivilprozessordnungen geregelt.[184]

b) Fremdwährungen

Lautet eine Geldforderung nicht auf Franken, ist sie gemäss Art. 67 Abs. 1 Ziff. 3 SchKG umzurechnen und im Betreibungsbegehren in «gesetzlicher Schweizerwährung» anzugeben. Dasselbe gilt für das Fortsetzungsbegehren.[185] Auch Rechtsöffnung wird nur für eine Forderung in Franken gewährt. Die vorgeschriebene Umrechnung in Franken ist eine Regel des schweizerischen *ordre public*.[186] Die Umrechnung ist vollstreckungsrechtlicher Natur. Es wird keine neue Forderung, welche auf Franken lautet, begründet.[187] Folglich kann der Schuldner während des Betreibungsverfahrens die Schuld weiterhin in der ursprünglichen Fremdwährung erfüllen.[188]

Für die Umrechnung ist der Kurs des Devisenangebots am Tag des Betreibungsbegehrens massgeblich. Die Gläubigerin kann nicht alternativ den Kurs bei Fälligkeit der Forderung wählen.[189] Die Wahlmöglichkeit von Art. 84 Abs. 2 OR findet keine Anwendung. Steigt der Kurs der Fremdwährung nach der Einreichung des Betreibungsbegehrens, kann die Gläubigerin den dadurch erlittenen Schaden nachfordern, muss hierfür jedoch eine neue Betreibung einleiten.[190] Überdies erlaubt Art. 88 Abs. 4 SchKG der Gläubigerin, im Zeitpunkt des Fortsetzungsbegehrens eine erneute Umrechnung der

183 Schweizerische Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008 (SR 272).

184 Vgl. BSK SchKG-ACOCELLA, Art. 38 N 1 m.w.H. Der Vorschlag, auch die Vollstreckung anderer Ansprüche mit Angabe eines Geldwerts in das SchKG aufzunehmen, war seinerzeit vom Parlament verworfen worden.

185 BGE 94 III 74 E. 3 S. 76.

186 BGE 137 III 623 E. 3 S. 624.

187 BK OR-WEBER, Art. 84 N 349 m.w.H. (keine Novation gemäss Art. 116 OR).

188 Dabei besteht wegen der Kursschwankungen das Risiko, dass der Schuldner im Vergleich zu dem in Betreibung gesetzten Betrag in Franken zu viel oder zu wenig leistet, vgl. BSK SchKG-ACOCELLA, Art. 38 N 10 m.w.H.

189 BGE 137 III 623 E. 3 S. 624 f. (Rechtskraft des Scheidungsurteils als Stichtag für Umrechnung der Forderung von Pfund in Franken verletzt Bundesrecht).

190 BK OR-WEBER, Art. 84 N 354 m.w.H. Bezahlt der Schuldner mehr als ursprünglich geschuldet, kann er gestützt auf Art. 86 SchKG eine Rückforderungsklage erheben.

Forderungssumme zum aktuellen Kurs zu verlangen. Im Konkurs wird die Forderung am Tag der Konkurseröffnung umgerechnet.[191]

Der Umrechnungskurs einer Fremdwährung in Franken ist gemäss Bundesgericht eine notorische Tatsache, welche von der Betreibungsgläubigerin nicht bewiesen werden muss.[192] Das Bundesgericht stellt auf die Website <http://fxtop.com> ab, welche die offiziellen Kurse der Europäischen Zentralbank wiedergeben soll.[193] Es handelt sich um eine private Website, die von der französischen Gesellschaft FXTOP sàrl betrieben wird und sich gemäss Selbstdeklaration bei kleineren Währungen auch auf andere Quellen stützt.[194] Auf der Webseite können auf einfache und eindeutige Weise die Umrechnungskurse auch für weit zurückliegende Daten abgefragt werden. Will die Gläubigerin einen davon abweichenden Brief-, Devisen- oder Notenkurs zur Anwendung bringen, hat sie diesen mit der Einreichung des Rechtsöffnungsbegehrens zu belegen. Die auf <www.oanda.com> und <www.snb.ch> veröffentlichten Interbanken-Devisenkurse geben einen Mittelkurs zwischen Brief- und Geldkurs wieder und gelten deshalb zumeist als nicht geeignet.[195]

Haben die Parteien eine Effektivklausel vereinbart, lässt sich die Fremdwährungsschuld nicht durch Schuldbetreibung, sondern einzig mit der Realvollstreckung nach Art. 335 ff. ZPO eintreiben.[196] Es wird von einer Sachschuld ausgegangen.[197]

c) WIR

Forderungen in WIR werden nicht als Geldforderungen behandelt und sind folglich gemäss der Zivilprozessordnung durchzusetzen.[198] Ihre Vollstreckung im Betreibungsverfahren ist möglich, wenn ein Urteil oder ein gerichtlicher Vergleich die Forderungssumme in Franken ausweisen oder

---

191 BK OR-WEBER, Art. 84 N 356. Die Umrechnung gemäss dem Zeitpunkt der Konkurseröffnung kann etwa bei der Insolvenz einer Handelsplattform angesichts der Wertschwankungen zu stossenden Ergebnissen führen.

192 BGE 135 III 88 E. 4.1 S. 90. Offenbleibt, inwiefern sich diese Annahme auch für wenig verbreitete Fremdwährungen rechtfertigt.

193 BGE 137 III 623 E. 3 S. 625.

194 Vgl. <http://fxtop.com/en/rules.php#source>.

195 BSK SchKG-STAEHELIN, Art. 80 N 52.

196 BSK SchKG-ACOCELLA, Art. 38 N 10 m.w.H.

197 BK ZPO-KELLERHALS, Art. 335 N 30.

198 BK ZPO-KELLERHALS, Art. 335 N 30.

zumindest den Umrechnungskurs zahlenmässig genau festlegen.[199] Denn der Entscheid über die Höhe der in Betreibung gesetzten Forderung soll dem Gericht vorbehalten bleiben und nicht durch die Betreibungsbehörden gefällt werden können.[200] Das WIR-System sieht ein Umtauschverbot vor; ein objektiver Umrechnungskurs ist nicht vorhanden. Das Umtauschverbot ist vergleichbar mit einer Effektivklausel, weshalb grundsätzlich die Realexekution zur Anwendung gelangt.

d) Virtuelle Währungen

aa) Schuld in staatlicher Währung

Eine Betreibung ist unzweifelhaft möglich, soweit eine Schuld in einer Fremdwährung oder in Franken besteht. Dienen virtuelle Währungen als Zahlungsmittel und ist der Preis für die erworbene Ware oder Dienstleistung in einer staatlichen Währung festgesetzt worden, lautet die ursprüngliche Schuld auf die staatliche Währung. Damit kann die Schuldbetreibung auf der Basis der staatlichen Währung – bei einer Fremdwährung umgerechnet in Franken – durchgeführt werden (vgl. vorne, III.1.b). Die Situation ist ähnlich wie bei einer WIR-Schuld, falls die Leistung in WIR fehlgeschlagen oder der Schuldner erfolglos gemahnt worden ist (vorne, bei Fn. 163).

Wird der Preis zwar in virtueller Währung angegeben, aber gleichzeitig ein Umrechnungskurs oder ein Betrag in staatlicher Währung erwähnt, kann dies ein Indiz für die Begründung beziehungsweise Anerkennung einer Schuld in der staatlichen Währung darstellen. Die entsprechende obligationenrechtliche Vorfrage ist durch Auslegung zu klären. Eine Schuld in Franken lässt sich auch bloss im Sinne einer Suspensivbedingung für den Verzugs- oder Vollstreckungsfall vereinbaren. Liegt demgegenüber eine Währungsoptions- oder Alternativwährungsklausel vor und wählt der Schuldner beziehungsweise die Gläubigerin die Erfüllung in virtueller Währung, fehlt es an einer Schuld in der staatlichen Währung.

---

199 BGE 94 III 74 E. 3 S. 76 (die Fortsetzung der Betreibung ist nicht möglich, wenn die Umrechnung gemäss dem Urteil oder Vergleich zu einem erst noch zu ermittelnden Kurs erfolgen soll; Übergabe von WIR-Checks als Sachleistung); BSK SchKG-ACOCELLA, Art. 38 N 11 m.w.H.

200 BGE 94 III 74 E. 3 S. 77.

bb) Umrechnung

Die Umrechnung der Schuld in Franken ist für die Betreibung aus theoretischer wie praktischer Sicht zentral. Den Betreibungsbehörden sollte bei der Bestimmung der Höhe der Forderungssumme kein Ermessen zukommen. Im Streitfall müsste der Schuldner Rechtsvorschlag erheben und die Gläubigerin vor dem Rechtsöffnungsgericht den massgeblichen Umrechnungskurs nachweisen. Dem Rechtsöffnungsgericht obliegt der Entscheid über die Rechtmässigkeit der Umrechnung auch in Fällen, in denen das zugrunde liegende Urteil auf eine Fremdwährung lautet.[201] Ist die Umrechnung nicht genügend dokumentiert, kann die Rechtsöffnung verweigert werden.

Auf die Volatilität bei virtuellen Währungen (vorne, bei Fn. 50) und die unterschiedlichen Handelsplattformen (vorne, II.2) ist bereits hingewiesen worden. Offizielle Umrechnungskurse existieren nicht. Keine der Plattformen geniesst derzeit eine höhere Autorität als die anderen.[202] Als «notorische Tatsache» (vorne, bei Fn. 192) lassen sich die Kurse nicht betrachten. Dies spricht gegen die Möglichkeit einer Betreibung.[203] Immerhin lässt sich anhand der Konsultation der Kurse mehrerer Plattformen bei den verbreiteten virtuellen Währungen ein Kurs annäherungsweise bestimmen.[204] Darauf ist im Zusammenhang mit der Verrechnung von Forderungen hingewiesen worden (vorne, bei Fn. 150). Zu ergänzen ist, dass die vom Bundesgericht für Fremdwährungen als massgeblich erachtete Website <http://fxtop.com> (vorne, bei Fn. 193) Bitcoin berücksichtigt und historische Umrechnungskurse anzeigt.[205]

cc) Zulässigkeit der Betreibung

Beim Erwerb von virtuellen Währungen über eine Plattform möchte die Gläubigerin die Währungseinheiten erhalten, um diese als Zahlungsmittel oder zu Anlagezwecken nutzen zu können. Die staatliche Währung wird als Entgelt eingesetzt, wie beim Geldwechselgeschäft üblich. Eine Umrechnung und Vollstreckung in Franken wäre nicht sinnvoll. Insoweit ist von einer

---

201 BSK SchKG-STAEHELIN, Art. 80 N 52.

202 MIGNON, Jusletter 4. Mai 2015, Rz. 197.

203 Ähnlich SCHMID/SCHMID, Jusletter 4. Juni 2012, Rz. 30 (hinsichtlich Bitcoin).

204 Demgegenüber existiert bei WIR aufgrund des Umtauschverbots kein Kurs. Die Umrechnung erfolgt jeweils 1:1 (vorne, bei Fn. 163).

205 Vgl. <http://fxtop.com/en/historical-exchange-rates.php?MA=1>. Bitcoin wird in der Liste unter der Abkürzung «XBT» geführt.

Sachleistung auszugehen, deren Realexekution der Zivilprozessordnung untersteht.

Auch sonstige Schulden, welche ausschliesslich auf eine virtuelle Währung lauten, sind grundsätzlich als Sachleistungen zu vollstrecken. Es ist die Vereinbarung der effektiven Leistung in virtueller Währung zu vermuten (vorne, I.5.a.cc). Die Realexekution gilt erst recht für virtuelle Währungen, welche nicht häufig gehandelt werden und bei denen es schwierig ist, einen Umrechnungskurs zu bestimmen. Vorbehalten bleibt der Fall, dass ein Urteil beziehungsweise ein gerichtlicher Vergleich den geschuldeten Betrag in Franken ausweist oder den Umrechnungskurs exakt angibt (vorne, bei Fn. 199). Bei *stable coins* (vorne, I.2.e.ee), deren Wert an eine staatliche Währung gebunden ist, rechtfertigt die Verwandtschaft mit Fremdwährungen die Anwendung des Schuldbetreibungsverfahrens.[206] Der Umrechnungskurs dürfte sich regelmässig ohne grössere Schwierigkeiten bestimmen lassen. Vorbehalten bleibt wiederum die ausdrückliche oder konkludente Vereinbarung der effektiven Leistung.

Verschiedentlich wird in der Lehre die Betreibung für möglich gehalten, sofern die Parteien einen Umrechnungskurs festgelegt beziehungsweise die massgebliche Plattform spezifiziert haben.[207] Dadurch können die praktischen Schwierigkeiten bei der Bestimmung der Forderungssumme in Franken ausgeräumt oder zumindest reduziert werden. Doch ist zu bedenken, dass die Umrechnung in Franken im Rahmen der Betreibung ein vollstreckungsrechtlicher Akt zwingender Natur ist (vorne, bei Fn. 186), welcher der Parteidisposition entzogen ist. Soweit zur Begründung auf Gerichtsurteile zu WIR verwiesen wird,[208] ist daran zu erinnern, dass diesen Fällen regelmässig eine in WIR zahlbare Schuld in Franken zugrunde liegt und ausserdem die Besonderheiten zu beachten sind, welche sich aus den Allgemeinen Geschäfts- und Teilnahmebedingungen der WIR Bank Genossenschaft ergeben.

---

206 Gewisse Abweichungen vom Kurs der staatlichen Währung (vgl. etwa zum *tether* vorne, Fn. 57) stehen der Anwendung des Betreibungsverfahrens nicht entgegen.

207 SCHMID/SCHMID, Jusletter 4. Juni 2012, Rz. 30; ihnen folgend MIGNON, Jusletter 4. Mai 2015, Rz. 197; ebenso GOBAT, AJP 2016, S. 1099.

208 Etwa Entscheid der Obergerichtskommission des Kantons Obwalden vom 17. Juni 2005, Amtsbericht über die Rechtspflege des Kantons Obwalden 2004/05, Nr. 22, S. 103.

dd) Realexekution

Die Durchsetzung einer Forderung in virtueller Währung im Realvollstreckungsverfahren gemäss Art. 335 ff. ZPO kann daran scheitern, dass sich der Schuldner weigert, die Übertragung der virtuellen Währungseinheiten mittels seines privaten Schlüssels auszulösen. Anders als bei einem Bankkonto hat der Inhaber eines privaten Schlüssels die alleinige Verfügungsmacht über die damit verbundenen Werteinheiten auf der Blockchain. Kommt der Schuldner den gerichtlichen Anordnungen nicht nach, kann die Gläubigerin gemäss Art. 345 Abs. 1 ZPO Schadenersatz[209] beziehungsweise die Umwandlung der geschuldeten Leistung in eine Geldleistung (Taxation) verlangen. Die Gläubigerin muss hierfür den Geldwert der nicht erfüllten Realleistung darlegen.[210] Den relevanten Umrechnungskurs setzt das Vollstreckungsgericht gestützt auf Art. 345 Abs. 2 ZPO endgültig fest. Der Taxationsentscheid ist ein definitiver Rechtsöffnungstitel im Sinne von Art. 80 Abs. 1 SchKG. Der Schuldner kann bis zur Tilgung der Schuld weiterhin realiter erfüllen. Folglich steht auch bei der Realexekution noch die Zwangsvollstreckung in Geld zur Verfügung, doch stellt die Schuldbetreibung aus prozessökonomischer Sicht der direktere Weg dar.

2. Pfändung und Sicherung

a) Geltungsbereich und Qualifikation

In diesem Abschnitt wird erörtert, ob virtuelle Währungseinheiten Gegenstand einer Pfändung oder von Sicherungsmassnahmen bilden können. Soll demgegenüber für eine Forderung in virtueller Währung die Pfändung oder Sicherungsmassnahmen verlangt werden, kann auf die obigen Ausführungen verwiesen werden (vorne, IV.1). Wie das Betreibungs- und das Fortsetzungsbegehren muss auch ein *Arrestbegehren* auf Franken lauten.[211] Ist die Betreibung bereits eingeleitet worden, wird der Umrechnungsbetrag übernommen. Ansonsten erfolgt die Umrechnung im Zeitpunkt der Einreichung des Arrestbegehrens.[212]

---

209 Es geht nicht um klassischen Schadenersatz, sondern um den Vermögensausgleich im Wert der Primärleistung im Zeitpunkt der Urteilsfällung, vgl. BK ZPO-KELLERHALS, Art. 345 N 15 und 17 m.w.H.

210 BK ZPO-KELLERHALS, Art. 345 N 12.

211 BK OR-WEBER, Art. 84 N 362.

212 BGer Urteil 5A_197/2012 vom 26. September 2012 E. 2.1.

Grundsätzlich sind sämtliche Vermögenswerte pfändbar, sofern nicht eine der Ausnahmen von Art. 92 f. SchKG greift. Auch Guthaben in WIR lassen sich gemäss der Rechtsprechung pfänden.[213] Aus rechtlicher Sicht spricht nichts gegen die Pfändbarkeit virtueller Währungen. Dasselbe gilt für einen Arrest, welcher auf virtuelle Währungseinheiten gelegt wird. Für den Arrestvollzug gelten Art. 91–109 SchKG über die Pfändung sinngemäss (Art. 275 SchKG). Nach Art. 91 Abs. 1 Ziff. 2 SchKG ist der Schuldner verpflichtet, die ihm gehörenden Vermögensgegenstände sowie seine Forderungen und Rechte gegenüber Dritten anzugeben, damit das Betreibungsamt die Pfändung vollziehen kann. Mit der Pfändungserklärung wird der Schuldner darauf hingewiesen, dass er über die gepfändeten Vermögenswerte nicht mehr verfügen darf (Art. 96 Abs. 1 SchKG). Zusätzlich sieht das Gesetz vor, dass der Betreibungsbeamte Massnahmen zur Sicherung des Vermögens trifft. Kostbare bewegliche Sachen wie Geld, Banknoten, Inhaberpapiere oder Edelmetalle werden gemäss Art. 98 Abs. 1 SchKG durch das Betreibungsamt verwahrt. Dasselbe gilt für weitere Gegenstände, wenn der Betreibungsbeamte es für angemessen erachtet (Art. 98 Abs. 3 SchKG). Zur Absicherung wird Drittschuldnern von gepfändeten Forderungen nach Art. 99 SchKG angezeigt, dass sie ihre Leistung an das Betreibungsamt erbringen müssen.

Die Pfändung von virtuellen Währungseinheiten hängt von der technischen Ausgestaltung der Verwahrung sowie teilweise von der rechtlichen Qualifikation ab. Die Werteinheiten als solche befinden sich nicht bei ihrem Inhaber, sondern werden – zumindest bei dezentralen virtuellen Währungen – im Computer-Netzwerk abgebildet (vorne, bei Fn. 46). Eine Forderung liegt typischerweise mangels Gegenpartei nicht vor, ebenso wenig beziehungsweise höchstens indirekt als Zugriffsinstrument eine körperliche Sache in klassischem Sinne, beispielsweise eine Bitcoin-Münze, auf welcher ein privater Schlüssel abgebildet ist. Nachfolgend wird danach differenziert, ob dem Schuldner mittels seines privaten Schlüssels Verfügungsmacht über die Werteinheiten (IV.2.b) oder ob ihm lediglich ein vertragliches Recht auf virtuelle Währungseinheiten beziehungsweise den dazugehörigen privaten Schlüssel zukommt (IV.2.c).

213 BGer Urteil 5C.268/2002 vom 14. Februar 2003 E. 2.3.

b) Verfügungsmacht über private Schlüssel

Bei einem *software* oder *desktop wallet* installiert der Schuldner eine Software auf seinem Computer. Der private Schlüssel wird auf diese Weise lokal auf der Festplatte des Computers verschlüsselt gespeichert. Hier liegt es nahe, den gesamten Computer in Verwahrung zu nehmen, weil dieser gewissermassen das Zugriffsinstrument zu den virtuellen Währungseinheiten verkörpert. Rechtlich darf der Computer hierfür nicht gemäss Art. 92 Abs. 1 Ziff. 1 SchKG zu den unentbehrlichen Vermögensgegenständen des persönlichen Gebrauchs des Schuldners und von dessen Familie gehören. Technisch betrachtet ist das Betreibungsamt auf die Mitwirkung des Schuldners angewiesen, sofern der Computer mit einem Passwort geschützt ist. Erlangt der Betreibungsbeamte auf diese Weise Zugriff, kann er den Computer gestützt auf Art. 98 Abs. 3 SchKG in amtliche Verwahrung nehmen.[214] Damit der Schuldner nicht mit einer etwaigen Kopie des privaten Schlüssels weiterhin Zugriff auf sein Wallet nimmt, sollte das Betreibungsamt die Währungseinheiten sicherungshalber umgehend auf ein Wallet transferieren, auf welches der Schuldner keinen Zugriff hat. Die Befugnis zu einer solchen Überweisung lässt sich zwar nicht ausdrücklich auf das Gesetz stützen, entspricht aber der Inbesitznahme von physischen Vermögenswerten durch das Betreibungsamt. Sind die virtuellen Währungseinheiten übertragen worden, erübrigt sich die amtliche Verwahrung des Computers des Schuldners.

Ein *hardware wallet*, das heisst ein spezielles Speichermedium ähnlich einem USB-Stick, worauf der private Schlüssel abgespeichert wird, stellt eine bewegliche Sache gemäss Art. 98 Abs. 3 SchKG dar. Dieses kann vom Betreibungsamt in Verwahrung genommen werden. Dasselbe gilt für andere Formen des *cold storage,* das heisst der Aufbewahrung des privaten Schlüssels *offline*, etwa auf einem Blatt Papier *(paper wallet)*.[215] Wiederum ist es für das Amt empfehlenswert, die virtuellen Währungseinheiten auf eine neue Adresse zu übertragen. Wird der private Schlüssel vom Schuldner mittels *online wallet* auf dem Server der Betreiberin einer Handelsplattform verwahrt und verfügt das Betreibungsamt über die Zugriffsdaten, ist ebenfalls eine Übertragung auf ein anderes Wallet denkbar. Die Möglichkeit einer physischen Verwahrung durch das Amt scheidet hier aus.

---

214 Für Anwendung von Art. 98 Abs. 1 SchKG auf Bitcoin PILLER, AJP 2017, S. 1436.

215 Hierzu JACQUEMART/MEYER, GesKR 2017, S. 471.

Komplexer sind Konstellationen, in denen die Währungseinheiten zum Schutz vor Missbrauch auf einem *multi-signature wallet* abgespeichert sind.[216] In diesem Fall kann nur mit einer Mehrzahl von privaten Schlüsseln auf die Vermögenswerte zugegriffen werden. Üblicherweise werden zur gültigen Signatur einer Transaktion zwei von drei oder fünf von sieben Schlüsseln benötigt. Sofern die Währungseinheiten der Vermögensmasse des Schuldners zuzuordnen sind und die Schlüssel bei Dritten aufbewahrt werden, fragt sich, ob diese Dritten zur Mitwirkung verpflichtet werden können. Gemäss Art. 91 Abs. 4 SchKG sind Dritte, welche Vermögensgegenstände des Schuldners verwahren oder bei denen er Guthaben hat, in gleichem Umfang auskunftspflichtig wie der Schuldner. Nach der Rechtsprechung sind sie überdies verpflichtet, Räume und Behältnisse zu öffnen und gegebenenfalls deren zwangsweise Öffnung zu dulden, wenn der Schuldner dort wohnt oder Vermögensstücke aufbewahrt.[217] Gestützt auf diese Rechtsprechung wird von Dritten verlangt werden können, Datenträger mit privaten Schlüsseln herauszugeben oder an der Übertragung von Währungseinheiten des Schuldners mitzuwirken.

c) Vertraglicher Anspruch auf virtuelle Währungen

Nicht immer halten Inhaber virtueller Währungseinheiten als direktes Zugriffsinstrument einen privaten Schlüssel. Einerseits steht ihnen vielfach bloss eine Forderung auf Auslieferung virtueller Währungen zu. Anderseits lassen sich private Schlüssel über spezialisierte, als besonders sicher geltende Dienstleister (*Vault*-Anbieter) verwalten.[218]

Bei vielen der verbreiteten Plattformen für virtuelle Währungen hat die Inhaberin von Währungseinheiten keinen direkten Zugriff mittels eines privaten Schlüssels, sondern bloss einen Anspruch gegenüber der Anbieterin auf Auslieferung ihrer virtuellen Währungseinheiten.[219] Die Währungseinheiten werden von der Anbieterin in *Sammel-Wallets* verwahrt, ähnlich einem Omnibus-Konto. Dadurch können Kauf- und Verkaufsangebote miteinander verbunden werden, ohne dass die Transaktionen über die Block-

[216] Vgl. JACQUEMART/MEYER, GesKR 2017, S. 471.

[217] Vgl. BGE 66 III 30 S. 32 f.; 102 III 6 E. 2 S. 8 f. (zwangsweise Öffnung des vom Schuldner bei einer Bank gemieteten Tresorfachs im Rahmen einer provisorischen Pfändung).

[218] Zum Beispiel Xapo, <https://xapo.com/vault>.

[219] Näher zu derartigen «Sammelkonten» MAURENBRECHER/MEIER, Jusletter 4. Dezember 2017, Rz. 11.

chain abgewickelt und hierfür Gebühren anfallen. Die Nutzerin gibt wie beim E-Banking eine Transaktion in Auftrag, indem sie sich mittels eines Benutzernamens und eines Passworts auf ihrem Online-Konto anmeldet und die Transaktion autorisiert.

Bei dieser Struktur lassen sich die virtuellen Währungseinheiten rechtlich nicht ohne Weiteres dem Schuldner zuordnen. Vielmehr wird dieser häufig bloss über eine Forderung gegenüber der Betreiberin der Handelsplattform verfügen. Letztere ist gegenüber dem Betreibungsamt auskunftspflichtig. Wird die Forderung gepfändet, ist der Handelsplattform gemäss Art. 99 SchKG anzuzeigen, dass sie an das Betreibungsamt zu leisten hat. Erschwerend kommt hinzu, dass die meisten Handelsplattformen ihren Sitz im Ausland haben. Dies bedeutet, dass die Zustellung statt per Post je nach ausländischem Recht unter Umständen rechtshilfeweise zu erfolgen hat und dass im Ausland domizilierte Drittschuldner nicht zur Anerkennung der Pfändung gezwungen werden können.[220] Eine Pflicht des Schuldners, unter Nutzung seiner Kontozugangsdaten eine Übertragung der Währungseinheiten in den Verfügungsbereich des Betreibungsamts auszulösen, lässt sich aus dem Gesetz nicht ableiten. Doch macht sich der Schuldner strafbar, falls er anderweitig über die gepfändeten Vermögenswerte verfügt. Unbestrittene fällige Forderungen des Schuldners gegenüber Dritten hat das Betreibungsamt ab dem Vollzug der Pfändung gestützt auf Art. 100 SchKG einzuziehen.[221] Dies gilt auch für Forderungen auf virtuelle Währungen.

Lässt die Inhaberin von virtuellen Währungseinheiten ihren privaten Schlüssel bei einem *Vault*-Anbieter aufbewahren, ist dieser als Drittverwahrer gestützt auf die Praxis zu Art. 91 Abs. 4 SchKG (vorne, bei Fn. 217) verpflichtet, dem Betreibungsamt Zugriff auf den privaten Schlüssel zu gewähren. Die Situation ist vergleichbar mit einer Bank, welche das Tresorfach eines Kunden öffnen muss. Die besagte Bestimmung ist nicht auf körperliche Gegenstände beschränkt, sodass die rechtliche Qualifikation der Währungseinheit beziehungsweise des privaten Schlüssels nicht näher erörtert zu werden braucht. Ein ähnliches Resultat wird erzielt, wenn der Rückübertragungsanspruch des Schuldners gegenüber dem *Vault*-Anbieter als Forderung betrachtet wird, zu deren Geltendmachung das Betreibungsamt gestützt auf Art. 100 SchKG (vorne, bei Fn. 221) befugt ist.

---

220 BSK SchKG-LEBRECHT, Art. 99 N 5 m.w.H.

221 BSK SchKG-LEBRECHT, Art. 100 N 8.

3. Verwertung

Das Gesetz unterscheidet zwischen der Verwertung von beweglichen Sachen sowie Forderungen einerseits (Art. 122 ff. SchKG) und derjenigen von «Vermögensbestandteile[n] anderer Art», namentlich einer Nutzniessung oder von Anteilen an einem gemeinschaftlichen Vermögen, sowie von Immaterialgüterrechten anderseits (Art. 132 SchKG). Im letzteren Fall hat das Betreibungsamt die Aufsichtsbehörde um Bestimmung des anwendbaren Verfahrens zu ersuchen. Die Verwertung von Gesamthandanteilen wird in der Verordnung über die Pfändung und Verwertung von Anteilen an Gemeinschaftsvermögen (VVAG) vom 17. Januar 1923 (SR 281.41) näher geregelt. Auf Gemeinschaftskonten findet diese Verordnung keine Anwendung, sofern nicht Gesamteigentum vorliegt; vielmehr erfolgt die Rechtsausübung über das Widerspruchsverfahren.[222] Da es hier weder um Anteile an gemeinschaftlichem Vermögen noch um Immaterialgüterrechte geht, ist Art. 132 SchKG nicht anwendbar. Somit braucht das Betreibungsamt zur Bestimmung des Verfahrens nicht die Aufsichtsbehörde zu involvieren.[223]

Bei direkter Verfügungsmacht des Schuldners über den privaten Schlüssel besteht hinsichtlich der Währungseinheiten keine Forderung (vorne, IV.2.b). Unter Umständen kann mit Blick auf das verwendete Speichermedium oder eine ähnliche Hardware-Komponente eine bewegliche Sache angenommen werden. So oder anders rechtfertigt sich die zumindest analoge Anwendung von Art. 122 ff. SchKG.[224] Neben der ordentlichen Verwertungsart, der Versteigerung, kommt insbesondere der *Freihandverkauf* nach Art. 130 SchKG in Frage.[225] Liegt nicht das Einverständnis aller Beteiligten vor, ist hierfür grundsätzlich erforderlich, dass ein Markt- oder Börsenpreis existiert und der angebotene Preis dem Tageskurs entspricht (Art. 130 Ziff. 2 SchKG). Da gängige virtuelle Währungen über Plattformen gehandelt werden, gibt es trotz der hohen Tagesvolatilität (vorne, Fn. 152) einen Marktpreis.

Handelt es sich um eine noch ausstehende *Forderung* auf virtuelle Währungen, unterliegt deren Verwertung grundsätzlich denselben Regeln wie bewegliche Sachen.

---

222 BSK SchKG-RUTZ/ROTH, Art. 132 N 5 m.w.H.

223 A.M. PILLER, AJP 2017, S. 1436.

224 Für analoge Anwendung von Art. 122 ff. SchKG GOBAT, AJP 2016, S. 1103.

225 Gl.M. PILLER, AJP 2017, S. 1436.

V. Fazit

Der Versuch, virtuelle Währungen getreu der klassischen juristischen Methodik terminologisch einzuordnen und unter die in den obligationenrechtlichen Bestimmungen verwendeten Begriffe wie Geld und Geldschuld, Währung, Zahlungsmittel oder Zahlung zu subsumieren, erweist sich als unergiebig: Die Regeln aus dem analogen Zeitalter passen – selbst bei «analoger» Anwendung – nicht ohne Weiteres für digitale Sachverhalte. Dies verwundert kaum, da der Gesetzgeber die technologische Entwicklung nicht vorhersehen konnte. Es fehlt an einer klaren dogmatischen Terminologie und an eindeutigen Erscheinungsformen in der Praxis. Die Situation wird dadurch entschärft, dass die relevanten obligationenrechtlichen Bestimmungen mehrheitlich dispositiver Natur sind. Die massgeblichen Vorschriften sind jeweils gesondert zu prüfen. Auf diese Weise rücken die Umstände des Einzelfalls und etwaige Parteiabreden ins Zentrum. Eine kohärente privatrechtliche Einordnung virtueller Währungen lässt sich so nicht garantieren.

Soweit eine virtuelle Währung als Zahlungsmittel konzipiert ist – was nach hier vertretenem Verständnis begriffsnotwendig ist (vorne, bei Fn. 41) – und eine gewisse Verbreitung gefunden hat, ist es gerechtfertigt, die virtuelle Währung funktionell als Geld in weiterem Sinne und als Zahlungsmittel zu qualifizieren (vorne, bei Fn. 77). Eine generelle zivilrechtliche Gleichstellung mit einer klassischen *Fremdwährung* ist hingegen nicht angezeigt. Zu stark unterscheiden sich virtuelle Währungen vom herkömmlichen staatlichen Geld. Eine Behandlung als Fremdwährung käme höchstens in Frage, falls ein ausländischer Staat beziehungsweise eine Staatengemeinschaft eine virtuelle Währung nicht nur reguliert oder als zulässiges Zahlungsmittel anerkennt, sondern zu einer offiziellen Erscheinungsform der staatlichen Währung im Sinne eines *gesetzlichen* Zahlungsmittels mit Annahmeobliegenheit für Gläubigerinnen erhebt (vorne, I.4.d.gg). Dies dürfte früher oder später der Fall sein. Vermutlich wird der Staat hierfür eine eigene virtuelle Währung schaffen, welche im Ausland lediglich als «Fremdwährung» Einsatz findet. Es lässt sich aber nicht ausschliessen, dass gleichzeitig zwei Staaten dieselbe virtuelle Währung als gesetzliches Zahlungsmittel qualifizieren. Eine Fremdwährung ist aus Schweizer Sicht jedenfalls anzunehmen, wenn die von einem ausländischen Staat herausgegebene virtuelle Währung bloss eine digitalisierte Form der bestehenden staatlichen Währung darstellt.

Wie für eine klassische Geldschuld gilt auch für virtuelle Währungen das *Nennwertprinzip:* Wird bei der Entstehung der Schuld ein bestimmter Betrag festgesetzt, bleibt dieser massgeblich (vorne, Fn. 18). Eine Anpassung ge-

stützt auf die *clausula rebus sic stantibus* dürfte regelmässig an der Vorhersehbarkeit der Wertschwankungen virtueller Währungen scheitern (vorne, I.4.f).

Wird eine Schuld in virtueller Währung begründet, ist die Erfüllung in den entsprechenden Währungseinheiten zu erbringen – ähnlich wie es Art. 84 Abs. 1 OR für gesetzliche Zahlungsmittel statuiert (vorne, I.4.b). Dies sollte grundsätzlich auch nach einer durchgeführten Spaltung gelten. In welcher Währung eine Schuld erfüllt werden muss, richtet sich gemäss Art. 147 Abs. 3 IPRG nach Art. 84 Abs. 2 OR, sofern der vertraglich oder gesetzlich vorgesehene Zahlungsort in der Schweiz liegt. Erfolgt die Zahlung tatsächlich in der Schweiz, darf der Schuldner die Fremdwährungsschuld in Franken erfüllen, umgerechnet gemäss dem Zeitpunkt der Fälligkeit. Angesichts der erheblichen Unterschiede zwischen den derzeitigen virtuellen und staatlichen Währungen ist eine analoge Anwendung von *Art. 84 Abs. 2 OR* auf virtuelle Währungen im Regelfall nicht gerechtfertigt beziehungsweise es ist mangels gegenteiliger Abrede die Vereinbarung der effektiven Leistung in virtueller Währung zu vermuten (vorne, I.5.a.cc). Beim Erwerb von virtuellen Währungen über eine Handelsplattform oder zu Anlagezwecken versteht sich von selbst, dass die Gläubigerin die virtuellen Währungseinheiten und nicht die staatliche Währung, welche als Entgelt dient, erhalten möchte. Wird die virtuelle Währung hingegen als Zahlungsmittel eingesetzt, ergibt sich ein entsprechendes Wahlrecht regelmässig unabhängig von Art. 84 Abs. 2 OR: Ähnlich wie bei WIR wird der Preis zumeist in der staatlichen Währung angegeben und darauf hingewiesen, welche virtuellen Währungen von der Gläubigerin akzeptiert werden. Die ursprünglich geschuldete Leistung lautet auf die staatliche Währung, doch darf der Schuldner – mutmasslich erfüllungshalber und nicht an Zahlungs statt – auch virtuelle Währungseinheiten übertragen. Mangels gegenteiliger Vereinbarung rechtfertigt es sich, auf den Umrechnungskurs im Zeitpunkt der Leistung abzustellen.

Während der Erfüllungsort – in der Regel der Sitz oder Wohnsitz der Gläubigerin – aus technischen Gründen in einem dezentralen Computernetzwerk selten von praktischer Relevanz ist (vorne, I.5.c), erweist sich die Frage nach dem *Erfüllungszeitpunkt* als heikel (vorne, I.5.b). Bei gängigen virtuellen Währungen mit stark verteilter Rechenleistung ist die Wahrscheinlichkeit, dass eine Transaktion nicht akzeptiert oder rückgängig gemacht wird, nach ein paar Folgeblöcken gering. Die Schwelle der endgültigen Verfügungsmöglichkeit durch die Gläubigerin wird indessen nie

erreicht werden. Eine äusserst lang andauernde Erfüllungsobligation des Schuldners ohne Gefahrübergang wäre nicht vertretbar. Es erscheint zweckmässig, die Erfüllung der Schuld ohne anderslautende Parteivereinbarung dann zu bejahen, wenn die Transaktion mit sehr hoher Wahrscheinlichkeit gültig abgespeichert bleibt. Die dafür erforderliche Zeit und technischen Anforderungen variieren je nach der virtuellen Währung. Im Anschluss erlischt das Schuldverhältnis. Scheitert die Übertragung der virtuellen Währungseinheiten nachträglich doch noch, kann die Gläubigerin gegebenenfalls gestützt auf die ungerechtfertigte Bereicherung gegen den Schuldner oder Dritten vorgehen, welcher in den Besitz der virtuellen Währungseinheiten gelangt ist.

Die *Verrechnung* von Forderungen in unterschiedlichen virtuellen Währungen oder einer Forderung in virtueller Währung mit einer solchen in einer staatlichen Währung wird durch die Wertschwankungen, fehlende offizielle Umrechnungskurse und Preisdifferenzen zwischen einzelnen Handelsplattformen erschwert. Bei virtuellen Währungen mit einem hohen Handelsvolumen und starker Verbreitung liesse sich ein Kurs anhand des Tagesmittelkurses der grössten Plattformen bestimmen. Würde zeitlich auf den Zugang der Verrechnungserklärung abgestellt, wären bei Verwendung des Tagesmittelkurses im Nachhinein eine Um- und Abrechnung erforderlich. Angesichts der vielfältigen Schwierigkeiten und des Risikos einer Benachteiligung des Verrechnungsgegners ist bei virtuellen Währungen mangels gegenteiliger Abrede die Vereinbarung einer effektiven Leistung zu vermuten, sodass die Möglichkeit der Verrechnung insoweit entfällt (vorne, II.2).

Der *Verzugszins* will die Gläubigerin für die vorenthaltene Geldleistung und den vom Schuldner in der Zwischenzeit bezogenen Nutzen entschädigen. Die zinstragende Verwahrung von virtuellen Währungen ist zurzeit nicht üblich. Deshalb muten Verzugszinsen «systemwidrig» an; sie sind mangels Parteivereinbarung abzulehnen. Doch ist im Einzelfall zu prüfen, ob eine primäre oder alternative Schuld in staatlicher Währung besteht, für welche die Gläubigerin Verzugszinsen verlangen kann. Möglich ist der Ersatz von Kursverlusten und weiteren Schäden aufgrund von Art. 103 Abs. 1 OR, falls der Schuldner den Verzugseintritt verschuldet hat (vorne, III.1.a).

Dienen virtuelle Währungen als Entgelt und wird der Preis – ohne Verwendung einer *Währungsoptions-* oder *Alternativwährungsklausel* – ausschliesslich in der virtuellen Währung festgesetzt, kann die Gläubigerin mangels gegenteiliger Vereinbarung auch im Verzugsfall nicht die Leistung

in staatlicher Währung verlangen. Doch werden die Preise in der Praxis häufig in der staatlichen Währung festgesetzt und stellt die Zahlung in virtueller Währung für den Schuldner eine blosse Option dar. In diesem Fall kommt der Gläubigerin grundsätzlich eine Schuld in der staatlichen Währung zu (vorne, III.1.b).

Erweist sich die Erfüllung einer Schuld in virtueller Währung aus technischen Gründen nachträglich generell als *objektiv unmöglich*, gilt Art. 119 OR. Hingegen kann die Gläubigerin bei einer bloss *subjektiven* Unmöglichkeit an der Erfüllung ihrer Forderung festhalten und Schadenersatz verlangen (vorne, III.2).

Für die massgebliche Währung bei *Schadenersatzansprüchen* stellt die bisherige Gerichtspraxis auf den Schadensort oder die vertraglich vereinbarte Währung ab. Gerade bei virtuellen Währungen ist eine flexiblere Haltung angezeigt. Häufig wird es sich rechtfertigen, Schadenersatz in Franken zu gewähren, auch wenn dieser mit einer Schuld in virtueller Währung in Zusammenhang steht (vorne, III.3).

Die *Schuldbetreibung* wird ähnlich wie die Verrechnung durch das Problem der Bestimmung des Umrechnungskurses erschwert. Solange der Umrechnungskurs einer bestimmten virtuellen Währung für das Betreibungsamt nicht auf einfache und eindeutige Weise feststellbar ist, eignet sich die virtuelle Währung nicht für ein Betreibungsverfahren. Wiederum besteht bei der Verwendung als Zahlungsmittel häufig eine Schuld in staatlicher Währung, welche auf dem ordentlichen Weg in Betreibung gesetzt werden kann. Andernfalls ist die Situation vergleichbar mit einer Schuld in Fremdwährung unter Vereinbarung einer Effektivklausel. Insoweit ist von einer Sachleistung auszugehen, deren Realexekution sich nach Art. 335 ff. ZPO richtet. Gegenteiliges gilt, falls ein Urteil beziehungsweise gerichtlicher Vergleich den Betrag in Franken oder einen Umrechnungskurs angibt. Eine Parteivereinbarung zur Umrechnung genügt vollstreckungsrechtlich nicht, um die Zulässigkeit der Schuldbetreibung zu begründen, kann unter Umständen jedoch zivilrechtlich als Begründung beziehungsweise Anerkennung einer Schuld in der staatlichen Währung qualifiziert werden. Bei *stable coins* mit Bindung an eine staatliche Währung rechtfertigt die Verwandtschaft mit Fremdwährungen die Anwendung des Schuldbetreibungsverfahrens. Im Übrigen untersteht die Schuld in virtueller Währung der Realexekution. Scheitert diese an der renitenten Haltung des Schuldners, bleibt die Umwandlung der Schuld in eine Geldleistung gestützt auf Art. 345 Abs. 1 ZPO möglich (vorne, IV.1.d).

Virtuelle Währungen sind *pfändbar* und verarrestierbar. Je nach Art der Verwahrung und Zugriffsmöglichkeit wird der Betreibungsbeamte, welcher die Pfändung durchführt, den Computer des Schuldners oder entsprechende Speichermedien für private Schlüssel in amtliche Verwahrung nehmen. Zur Sicherheit sollten die Währungseinheiten rasch auf ein anderes Wallet übertragen werden, damit der Schuldner nicht mehr darüber verfügen kann. Kommt dem Schuldner bloss eine Forderung gegenüber der Betreiberin einer Plattform zu, ist diese Forderung zu pfänden und der Plattformbetreiberin anzuzeigen, dass sie ihre Leistung an das Betreibungsamt zu erbringen hat (vorne, IV.2). Sollen virtuelle Währungen *verwertet* werden, steht bei gängigen virtuellen Währungen mit einem Marktpreis der Freihandverkauf gemäss Art. 130 SchKG im Zentrum (vorne, IV.3).

Virtuelle Währungen stellen auch das Obligationenrecht vor vielfältige Herausforderungen. So naheliegend eine Qualifikation virtueller Währungen als Geld in weiterem Sinne – analog den herkömmlichen Fremdwährungen – zunächst erscheint: Eine nähere Betrachtung ergibt, dass sich virtuelle Währungen trotz vergleichbarer Funktionalität wesentlich von traditionellen Währungen unterscheiden. Institute wie die alternative Leistungsmöglichkeit in staatlicher Währung, die Verrechnung, der Verzugszins oder die Schuldbetreibung sind deshalb nicht ohne Weiteres anwendbar, sofern nicht eine Schuld in der staatlichen Währung existiert. Wie die Gerichts– und Behördenpraxis die Zahlung und den Verzug bei virtuellen Währungen beurteilt, wird sich zeigen. Aufgrund der dispositiven Natur zahlreicher obligationenrechtlicher Bestimmungen ist jedenfalls auf das konkrete Vertragsverhältnis sowie den Willen der Parteien abzustellen.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 1. Mai 2018.

ACOCELLA DOMENICO, Art. 38 SchKG, in: Daniel Staehelin/Thomas Bauer (Hrsg.), Basler Kommentar, Bundesgesetz über Schuldbetreibung und Konkurs I, Art. 1–158 SchKG, 2. Auflage, Basel 2010.

BÄRTSCHI HARALD/MEISSER CHRISTIAN, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich/Basel/Genf 2015, S. 113–160.

BREHM ROLAND, Berner Kommentar, Obligationenrecht, Die Entstehung durch unerlaubte Handlungen, Art. 41–61 OR, 4. Auflage, Bern 2013.

DASSER FELIX, Art. 147 IPRG, in: Heinrich Honsell u.a. (Hrsg.), Basler Kommentar, Internationales Privatrecht, 3. Auflage, Basel 2013.

EGGEN MIRJAM, Verträge über digitale Währungen, Eine privatrechtliche Qualifikation von Rechtsgeschäften in oder mit digitalen Währungen, Jusletter 4. Dezember 2017.

GOBAT SÉBASTIEN, Les monnaies virtuelles à l'épreuve de la LP, AJP 2016, S. 1095–1105.

JACQUEMART NICOLAS/MEYER STEPHAN D., Der Bitcoin-/Bitcoin-Cash-Hardfork, Die auftragsrechtliche Ablieferungspflicht bei Kryptowährungs-Dienstleistungen im Lichte der bundesgerichtlichen Rechtsprechung, GesKR 2017, S. 469–485.

KELLERHALS FRANZ, Berner Kommentar, Schweizerische Zivilprozessordnung, Band II, Art. 150–352 und Art. 400–406 ZPO, Bern 2012.

KESSLER MARTIN A., Art. 43 OR, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Auflage, Basel 2015.

KOLLER ALFRED, Haftung für Fremdwährungsschäden: Die massgebliche Währung, Anwaltsrevue 2017, S. 263–266.

KÜNG JOSEPH, Zahlung und Zahlungsort im internationalen Privatrecht, Ein Beitrag zur Vereinheitlichung des Geldrechts, Diss. Freiburg 1970.

LEBRECHT ANDRÉ E., Art. 99 und 100 SchKG, in: Daniel Staehelin/Thomas Bauer (Hrsg.), Basler Kommentar, Bundesgesetz über Schuldbetreibung und Konkurs I, Art. 1–158 SchKG, 2. Auflage, Basel 2010.

LEU URS, Art. 84 OR, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Auflage, Basel 2015.

LINDER THOMAS/MEYER STEPHAN D., Die steuerliche Behandlung von Bitcoin und anderen Kryptowährungen, Zürcher Steuerpraxis 2017, S. 191–210.

MAURENBRECHER BENEDIKT/MEIER URS, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, Jusletter 4. Dezember 2017.

MIGNON VINCENT, Le «[B]itcoin», un nouveau défi pour le juriste suisse?, Jusletter 4. Mai 2015.

PESCH PAULINA JO, Cryptocoin-Schulden, Haftung und Risikoverteilung bei der Verschaffung von Bitcoins und Alt-Coins, Diss. Münster, München 2017.

PETER WOLFGANG, Art. 120 OR, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Auflage, Basel 2015.

PILLER FRANÇOIS, Virtuelle Währungen – Reale Rechtsprobleme?, AJP 2017, S. 1426–1438.

RUTZ MAGDALENA/ROTH JÖRG, Art. 132 SchKG, in: Daniel Staehelin/Thomas Bauer (Hrsg.), Basler Kommentar, Bundesgesetz über Schuldbetreibung und Konkurs I, Art. 1–158 SchKG, 2. Auflage, Basel 2010.

SCHMID JEAN-DANIEL/SCHMID ALEXANDER, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, Jusletter 4. Juni 2012.

SCHRANER MARIUS, Zürcher Kommentar, Obligationenrecht, Teilband V/1e: Die Erfüllung der Obligationen, Art. 68–96 OR, 3. Auflage, Zürich/Basel/Genf 2000.

SCHULIN HERMANN, Art. 62 OR, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Auflage, Basel 2015.

STAEHELIN DANIEL, Art. 80 SchKG, in: Daniel Staehelin/Thomas Bauer (Hrsg.), Basler Kommentar, Bundesgesetz über Schuldbetreibung und Konkurs I, Art. 1–158 SchKG, 2. Auflage, Basel 2010.

VON WYSS FRIEDRICH, Die Schuldbetreibung nach schweizerischen Rechten, ZSR 1858, S. 3–114.

WEBER ROLF H., Berner Kommentar, Band VI: Obligationenrecht, 1. Abteilung: Allgemeine Bestimmungen, 4. Teilband: Die Erfüllung der Obligation, Art. 68–96 OR, 2. Auflage, Bern 2005.

– Berner Kommentar, Band VI: Obligationenrecht, 1. Abteilung: Allgemeine Bestimmungen, 5. Teilband: Die Folgen der Nichterfüllung, Art. 97–109 OR, Bern 2000.

– Elektronisches Geld, Erscheinungsformen und rechtlicher Problemaufriss, Zürich 1999.

WIEGAND WOLFGANG, Art. 97 OR, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 6. Auflage, Basel 2015.

ZELLWEGER-GUTKNECHT CORINNE, Digitale Landeswährung – Ein Überblick, Elektronisch gebuchte und staatlich gedeckte Einlagen als Zahlungsmittel, Jusletter 31. Oktober 2016.

– Berner Kommentar, Band VI: Obligationenrecht, 1. Abteilung: Allgemeine Bestimmungen, 7. Teilband: Das Erlöschen der Obligation, 2. Unterteilband: Verrechnung, Art. 120–126 OR, Bern 2012.

Materialien

Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, abrufbar unter: <www.newsd.admin.ch/newsd/message/attachments/35361.pdf> (zit. Bericht virtuelle Währungen).

Botschaft zu dem vom Bundesrathe am 23. Februar 1886 festgestellten Entwurfe eines Bundesgesetzes über Schuldbetreibung und Konkurs vom 6. April 1886, BBl 1886 II 1 ff. (zit. Botschaft SchKG).

Botschaft zum Bundesgesetz über das internationale Privatrecht (IPR-Gesetz) vom 10. November 1982, BBl 1983 I 263 ff. (zit. Botschaft IPRG).

Botschaft über einen neuen Geld- und Währungsartikel in der Bundesverfassung vom 27. Mai 1998, BBl 1998 IV 4007 ff. (zit. Botschaft Währungsartikel).

Botschaft zu einem Bundesgesetz über die Währung und die Zahlungsmittel (WZG) vom 26. Mai 1999, BBl 1999 7258 ff. (zit. Botschaft WZG).

Europäische Zentralbank, Stellungnahme der Europäischen Zentralbank vom 12. Oktober 2016 zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG (CON/2016/49), Amtsblatt der Europäischen Union vom 9. Dezember 2016, C 459/3–6, abrufbar unter: <www.ecb.europa.eu/ecb/legal/pdf/celex_52016ab0049_de_txt.pdf> (zit. EZB-Stellungnahme).

FINMA, Geldwäschereiverordnung-FINMA (GwV-FINMA), Erläuterungsbericht zur Totalrevision der GwV-FINMA vom 11. Februar 2015 (zit. Erläuterungsbericht FINMA).